SolarWinds

Storage Manager *powered by Profiler* Administrator Guide

Copyright © 1995-2012 SolarWinds Worldwide, LLC. All rights reserved worldwide.

No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, the SolarWinds & Design, ipMonitor, LANsurveyor, Orion, and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies. Microsoft®, Windows®, and SQL Server® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

SolarWinds Storage Manager powered by Profiler, 7-24-12

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Technical Support	www.solarwinds.com/support
User Forums	www.thwack.com

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including s and fields.
Italics	Book and CD titles, variable names, new terms
`Fixed font`	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [*value*]	Optional command parameters
Curly braces, as in {*value*}	Required command parameters
Logical OR, as in *value1*|*value2*	Exclusive command parameters where only one of the options can be specified

Storage Manager *powered by Profiler* Documentation

The following documents are included in the SolarWinds Storage Manager powered by Profiler documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Evaluation Guide	Provides an introduction to STM features and instructions for installation and initial configuration.
Page Help	Provides help for every window in the STM user interface
Release Notes	Provides the latest information about known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

Contents

About SolarWinds ..... *iii*

Contacting SolarWinds ..... *iii*

Conventions ..... *iii*

Storage Manager powered by Profiler Documentation ..... *iv*

Chapter 1

Introduction to SolarWinds Storage Manager *powered by Profiler* **1**

Why Install Storage Manager *1*

STM Architecture *3*

Chapter 2

Installation **6**

Storage Manager System Requirements *7*

Storage Manager Server *8*

Storage Manager Agents *9*

STM Application Module Requirements: *10*

STM Server Data Collector Ports Requirements *13*

Storage Manager Server Installation for Windows *14*

Downloading the Installer *15*

Installing Storage Manager over an Existing Profiler Deployment *16*

Clean Install of Storage Manager for Windows *16*

Installing the Storage Manager Integration Module on your Orion Server *18*

License Activation *18*

License Manager Page *20*

STM Agent OS Device Configuration *21*

STM Orion NPM Integration *23*

Storage Manager Database *24*

Chapter 3

Web Console Navigation **26**

Getting Started Page *29*

Managing User Accounts *29*

Discovering and Adding Devices *32*
Editing Devices *34*
Editing Devices *35*
Agent Status *36*
Data Retention Policies *37*

Chapter 4

Server Setup **38**

Chapter 5

Monitoring Storage Arrays **49**
Monitoring IBM 3xxx,4xxx,5xxx Arrays *58*
Monitoring EMC CLARiiON Arrays *62*
Monitoring NetApp Operations Manager *66*
Monitoring NetAPP Filer *69*
Monitoring Hitachi Data Systems *69*
3Par, Pillar, IBM SVC *69*
Monitoring Fibre Channel Devices *70*
Fibre Channel Switches Requirements *71*

Chapter 6

Backup Profiler **74**
Configuring the CA Arcserve *74*
Configuring CommVault Galaxy *77*
Configuring IBM TSM *79*
Configuring EMC Legato *83*
Configuring Symantec Backup Exec *84*
Configuring Symantec NetBackup *88*

Chapter 7

Monitoring VMware **90**
VMware Device Requirements *90*
Configuring VMware *93*

Application Monitoring *96*

Chapter 8

Reports and Schedules **101**

Creating a New Report *105*

Using Groups *112*

Chapter 9

Rules & Policies **117**

File Analysis Rule *119*

File Analysis on NAS and Virtual Machines *121*

Defining Threshold Rules *123*

SnapMirror Monitor *124*

Windows Event Log Rule *124*

Directory Analysis Rule *125*

Managing Rules *127*

Using External Scripts *130*

Policies *130*

Interacting with the thwack User Community *134*

Chapter 10

Linux Installation **135**

Backup Profiler Requirements *139*

Installing Agents on Windows Cluster (Windows 2008) *142*

Appendix

Appendix **146**

SMI-S Provider Installation & Configuration *146*
General SMI-S Questions *146*
SMI-S Providers *148*
Enabling SNMP *223*
SMI-S Provider Tools *263*
Remote Agent Upgrade Utility *273*
Performing an Agent Upgrade: *273*
How to enable SSL login for the STM website *274*
Installing Local Help Files *274*

General Troubleshooting..... 275

Index

Index 276

Chapter 1

Introduction to SolarWinds Storage Manager
powered by Profiler

SolarWinds Storage Manager (STM) is designed to give users greater control over their networked storage and server environments. Storage Manager supports event monitoring and reporting of the health, status, usage, and performance of critical storage and server devices. STM provides Web-accessible displays and reports that can be used by operators, administrators, and managers who are responsible for monitoring, allocating, upgrading and purchasing storage devices.

STM is composed of two separate components:

- STM Server: Collects data from agents, traps and pollers into a central database and distributes information to users via the web interface. Also allows the user to manage the Agents remotely.
- STM Agents: Provides the framework to gather the storage, server performance and file analysis information from devices (both local and remote) and transmits it to the STM server.

Why Install Storage Manager

Storage Manager provides accurate, critical classification and performance information for SAN, NAS, fibre channel switches and HBA's, enabling IT managers and administrators to monitor, alert, forecast, and act on both storage performance, utilization, and storage provisioning.

Collectively, Storage Manager powered by *Profiler* and Backup Profiler monitor a number of platforms, applications, and devices including the following devices:

Supported Devices

OS

- Linux
- Windows ®
- Unix (IBM AIX, HP-UX, Sun Solaris)
- Virtualization
- VMware ®
- Applications

- Oracle ®
- SQL Server ®
- Microsoft ® Exchange 2003
- Microsoft ® Exchange 2007

SAN and NAS:

- 3Par
- Dell™ EqualLogic™
- Dell PowerVault MD3000i
- Dell Compellent
- EMC Celerra ®
- EMC CLARiiON ® , VNX
- EMC Symmetrix DMX ,VMAX™
- EMC VNX
- Hitachi Data Systems ™
- HP StorageWorks EVA
- HP LeftHand P4000
- HP StorageWorks XP
- IBM® System Storage DS® 3xxx, 4xxx, 5xxx, 6xxx, 8xxx
- IBM System Storage™ N series
- IBMSystem Storage™ SANVolume Controller (SVC)
- IBM V7000
- NetApp®
- LSI™
- ONStor™
- Pillar
- SGI

Fibre Channel Switches and Fabric:

- Brocade Switches
- Cisco Switches
- McData

- QLogic switches
- Host Bus Adapters (HBAs) (Emulex® and QLogic)

Backup Profiler

Backup Profiler requires purchase and is licensed into two tiers.

Category 1: Backup Exec, Arcserve, Commvault

Category 2: Legato, TSM, Netbackup

Backup Profiler's web-based backup console provides your entire team with a real-time, at-a-glance view of all backup operations. It automatically summarizes backup status, exceptions, and trending of backup size. These functions make it easy for you to plan for growth, to ensure that your backup operations are compliant with regulations and corporate standards, and to prevent failed backups and loss of data.

Backup Profiler supports:

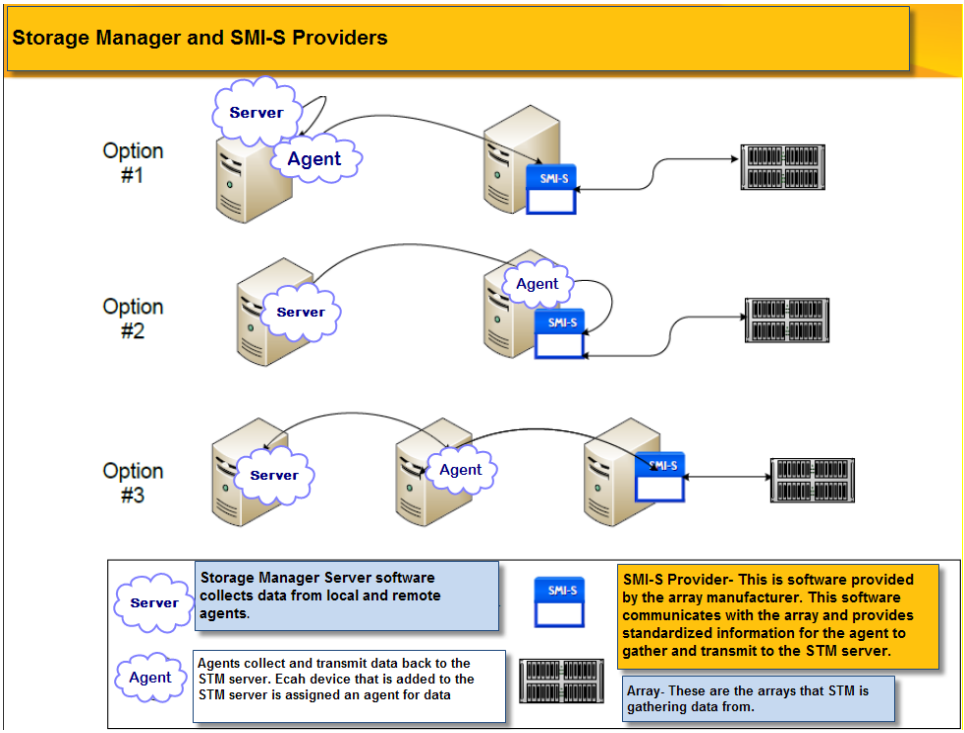
- Symantec/VERITAS NetBackup
- Symantec/VERITAS Backup Exec
- EMC Legato Networker
- IBM TSM
- CA BrightStor/ARCServe
- CommVault Galaxy

See the following sections for installation steps and system requirements:

- System Requirements
- Clean Install on a Windows Server
- Installing on an existing Profiler deployment
- Installing the Orion NPM Integration module
- License Activation
- Installing Agents
- Installing Agents on an Windows 2008 Cluster
- Linux Installation

STM Architecture

STM is comprised of a Server /Agent architecture.


Storage Manager and SMI-S Providers
Option #1
Server
Agent
SMI-S
Option #2
Server
Agent
SMI-S
Option #3
Server
Agent
SMI-S
Server
Storage Manager Server software collects data from local and remote agents.
SMI-S
SMI-S Provider- This is software provided by the array manufacturer. This software communicates with the array and provides standardized information for the agent to gather and transmit to the STM server.
Agent
Agents collect and transmit data back to the STM server. Ecah device that is added to the STM server is assigned an agent for data
Array- These are the arrays that STM is gathering data from.

STM Server

The STM server consists of a MySQL Database, Tomcat Web Server, Collector, Poller, Event Receiver, and a Maintenance process.

STM uses a variety of methods to collect data, both local and remote. STM can collect most data remotely, including storage arrays (NAS and SAN), VMware® hosts and virtual machines, Fibre Channel switches, databases (SQL and Oracle®) and file analysis.

For physical servers, backups and Exchange, agents are required on those servers. Some of the methods that STM uses to collect data includes: SMI-S, Telnet/SSH, SNMP, CIFS/NFS, API, WMI, SQL queries, Web Services, command line, and log parsing. Primary communication between the STM server and Agents occurs on ports 4319 TCP (HTTP) and 162 UDP (SNMP).

On Windows, the STM server consists of 6 services.

- MySQL
- Collector (Agent)
- Event Receiver
- Poller

- Maintenance
- Webserver

STM Agents

OS Agents reside on operating systems and provide two functions.

- • Agents gather asset, storage, performance and file information for that device.
- • Agents provide a platform to monitor applications or other devices that reside on or are connected to that server.

For more information about installing agents see:

- Installing Agents
- Installing Agents on an Windows 2008 Cluster

SMI-S Requirments

Storage Manager uses the Storage Management Initiative Specification (SMI-S) standard to discover and manage some of the devices it supports.

To determine if your device requires an SMI-S Prvodier to be installed see

SMI-S Provider section.

For more inofrmation as to which devices require SMI-S to be installed see the Provider Reference located.

http://www.solarwinds.com/documentation/profiler/docs/SMISProvider.pdf

Chapter 2

Installation

Storage Manager is composed of two separate components that will need to be installed. The server install and OS agents.

The following sections guide you through the various instalation scenarios for STM.

- System Requirements
- Clean Install on a Windows Server
- Installing on an existing Profiler deployment
- Installing the Orion NPM Integration module
- License Activation
- Installing Agents
- Installing Agents on an Windows 2008 Cluster
- Linux Installation
- SMI-S Provider Installation

Storage Manager System Requirements

Verify that you have downloaded the correct versions for your environment and that your system meets the minimum requirements.

System requirements are as follows:

- Server Requirements
- Agent Requirements
- Application Module Requirements
- VMware Requirements
- Fibre Channel Requirements
- Storage Device Port Requirements

Storage Manager Server

STM Server Operating System	Production : Windows 2003, 2008 (32 & 64 bit) Linux Red Hat, SUSE (32 & 64 bit)
Required Ports	Port 9000 as Web server port (HTTP) for the GUI. This port can be changed in the server.xml. Port 4319 as its communications port with STM Agents (HTTP). This port can be changed system wide, or on an agent by agent basis. Default SNMP port 162 (needs to change to 10162 if using Orion NPM)
Storage/Memory requirements	2 CPUs •Memory: 4 GB •Storage: 50 GB If you choose to install with less than 4GB, the STM Server may experience degraded performance.
STM Agents Operating System	Windows XP, Vista ,7 ,2000, 2003,2008
	AIX (PPC 32/64) - 5.0+ HP-UX PA-RISC -Itanium 11+ Linux (Intel-32, x86-64) - RedHat, SUSE Solaris (Sparc 32/64 bit) - 8,9,10 Solaris (Intel-32) - 10 Windows 2003, 2008, XP, Vista, 7 (32 & 64-bit.)

The install does NOT require a reboot.

Scenario Size Suggestions:

Small Installation: Up to 500 Disks

- Windows 32 or 64bit
- Dual Processor, 4 GB RAM
- 1 additional Agent per 200 VM
- Poller/agent: Single Processor, 1 GB of RAM

Medium Installation: Up to 3000 Disks

- Windows 64bit
- Quad Processor, 8-16 GB RAM

- 1 additional Agent per 200 VM
- Poller/agent: Single/Dual Processor, 2GB of RAM

Large Installation: Up to 30,000 disks

Windows 64bit

- 8-16 Processors, 16-64GB RAM
- 1 additional Agent per 200 VM
- Poller/agent: Single/Dual Processor, 4GB of RAM

Other System Requirements:

- Agent Requirements
- Application Module Requirements
- VMware Requirements
- Fibre Channel Requirements
- Port Requirements

Storage Manager Agents

The STM Data Collector/Agent can be installed on Windows, Linux, Solaris 8, 9 and 10, HP-UX 11.x, AIX 5.x.

Minimum Agent Requirements:

Monitoring just the server the agent is installed on:

- Ram – 512 MB
- CPU – (1) Pentium 4 or equivalent
- Free Hard Drive Space – 1GB

Monitoring a few Arrays, FC switches, and up to 200 VM:

- RAM – 4 or 6 GB
- Dual Core CPU
- Free Hard drive space – 1 GB

The Data collector/agent runs the following service/process

- STMAgent (Windows)
- STM_Agent (UNIX)

Primary Communication Ports:

- HTTP Port 4319 (configurable) – handles requests from STM Server Collector
- UDP Port 162 (configurable) – SNMP traps are sent to the STM Server

Credentials Required:

- Local System Account (Default)
- Log On rights of Domain Account if WMI counters/Logical disks are not accessible to Local System Account. Domain Account must belong to Local Administrators group.

Data Collector/OS Agent: Windows - File Analysis / Data Classification:

- Requires a Proxy Agent

Communication:

- Between proxy agent and STM Server, same as above
- CIFS between Proxy agent and Windows server

Credentials Required:

- File Scans: Domain Account with Log On rights with read access to CIFS targets
- CIFS Shares Discovery: Domain Account with Administrator privileges. CIFS targets for file scans can be added manually

Other System Requirements:

- Application Module Requirements
- VMware Requirements
- Fibre Channel Requirements
- Port Requirements

STM Application Module Requirements:

The following details the requirements of application modules you want to montior.

- Microsoft Exchange
- Microsoft SQL
- Oracle

Microsoft Exchange

Versions/Models	2003, 2007: Mailbox Analysis Server and Application Performance Attachment Analysis *(Ver. 2003 only)*
Requires Agent?	Yes – on Exchange Server (Ver. 2003 only) Yes – on Mailbox Server (Ver. 2007 only) No – on Hub transport and Client Servers (Ver. 2007 only)
Requires a Proxy Agent?	No
Prerequisites	Ver. 2003 • Create Domain user with Exchange View Only Administrator role defined • Define MAPI Profile for Domain user on Exchange Server, set as default Profile Ver. 2007 • Create Domain user with Exchange View Only Administrator role defined
Credentials	Run with Log On rights of Domain Account
Read/Write Actions	Read Only

Microsoft SQL:

Versions/Models	2000, 2005, 2008
Requires Agent?	No
Requires a Proxy Agent?	Yes – via STM Server
Prerequisites	Domain or Local DB user with: • Read-only access to ALL tables in the MASTER database • Permission to execute Stored Procedures • Permission to execute DBCC commands
Credentials	Account and password stored in STM database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	1433 or 1094 on MS SQL Server (depends on SQL configuration)

Communication	SQL Queries over IP

Oracle:

Versions/Models	10G, 11G
Requires Agent?	No
Requires a Proxy Agent?	Yes – via STM Server
Prerequisites	Requires ID with Table name Permissions V$SGASTAT select v$version select v$statname select v$sesstat select v$session select v$sysstat select dba_rollback_segs select dba_indexes select dba_tables select dba_segments select sys.dba_extents select sys.dba_data_files select sys.dba_tablespaces select sys.dba_free_space select V$OSSTAT select V$SYSMETRIC_HISTORY select
Credentials	Account and password stored in STM database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	Depends on Oracle configuration
Communication	SQL Queries over IP

Other System Requirements:

- VMware Requirements
- Fibre Channel Requirements
- Port Requirements

STM Server Data Collector Ports Requirements

SolarWinds Storage Manager requires the following ports:

- HTTP Port 4319 (configurable) – handles requests from Profiler Server Collector.
- UDP Port 162. By default if 162 is in use by Orion NPM for example, then Profiler will use 10162 or 20162 to register the agent, (also configurable) – SNMP traps are sent to the Profiler Server.

STM Web GUI Ports Requirements

- The Profiler web interface is contacted via HTTP (configurable HTTP or HTTPS) on Port 9000 (configurable).

STM Collector Ports Requirements

Handles the collection from STM Data Collectors/agents and also acts as a local data collector/agent. STM communicates with data collectors/agents on HTTP Port 4319 (configurable).

Application Module Requirements

- **Microsoft SQL** uses1433 or 1094 (depends on SQL configuration).

  STM for VMware

- **Virtual Center:** HTTPS Port 443.

  STM - Fiber Channel Switches

- **Cisco MDS, Brocade, McData,** and **QLogic Switches** use161 UDP on the switch.

Storage Device Ports Requirements

- **EMC Celerra:** Non-Configurable: 22 on the Control station.
- **NetApp:** 80 (HTTP)/443 (HTTPS) on NetApp head/cluster node and any available for CIFS/NFS.
- **3PAR:** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by 3PAR provider.
- **Dell EqualLogic:** 161 (UDP) on the EqualLogic Group IP.

- **EMC Symmetrix, DMX, VMAX:** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by **EMC Solutions Enabler.**
- **HP EVA:** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by HP CommandView.
- **HP MSA:** Non-configurable: 5989 (HTTPS) used by HP SMI-S Provider.
- **IBM DS 3K, 4K, 5K:** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by the SMI-S provider .Non-Configurable: 2463 used to set RPC sessions to the storage controller from SMI-S provider.
- **IBM DS 6K, 8K:** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider.
- **IBM SVC/V7000:** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider.
- **LSI:** Configurable 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider. Non-Configurable: 2463 used to set RPC sessions to the storage controller from SMI-S provider.
- **NetApp:** 80 (HTTP)/443 (HTTPS) on NetApp head/cluster node.
- **SUN/StorageTek:** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider. Non-Configurable: 2463 used to set RPC sessions to the storage controller from SMI-S provider

Storage Manager Server Installation for Windows

Before Installing: Close any services window(s). Installation will not work properly if you leave this window open during install.

- Ensure you have stopped your antivirus software. Some antivirus software packages have been found to interfere with the product installation.
- **Backup your database**: SolarWinds recommends backing up your database before performing any upgrades. See Backing up your Database for more information.

MySQL Notes: Uninstall any previous instances of MySQL. Only one instance of MySQL is supported at a time.

Installation Path: All STM binary and data files are located under the installation directory. When installing, select a directory located on a partition with enough space (we suggest 40 GB) to hold STM data files over time.

SolarWinds Virtualization Manager cannot be installed on the same server as Storage Manager.

Downloading the Installer

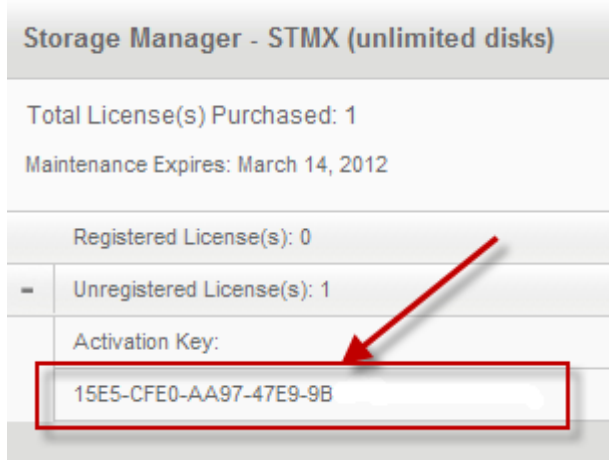
To download the Storage Manager installer, you will need your SolarWinds ID (SWID) and password to login into the customer portal.

Note: Existing customers received them in an email when Profiler was originally purchased. To obtain a SolarWinds ID (SWID) contact customer support.

The following steps detail how to download Storage Manager Server.

To Download the Storage Manager Server:

1. Login into the customer portal: http://www.solarwinds.com/customerportal/
2. Enter your SWID and password and click the **Log In** button.
3. Under downloads select the Storage Manager Server installer that is appropriate for your OS and then click DOWNLOAD ».
4. Click **View All** to list all available activation keys.
5. In each Storage Manager or Backup Profiler product section, copy the long string of characters under "**Activation Key**". The activation key will look similar to this. Copy it to clipboard for later use.



Before exiting the customer portal, download any Agent installers that are relevant to your deployment if needed.

Notes:

Which server download should I choose?

In general, choose the install that matches your OS and architecture. STM5.0 will handle 32bit to 64bit migrations of Profiler.

For example: If you install the 32bit version of Profiler on a 64bit system, download the STM5.0 64bit version and run the installer - it will automatically migrate 32bit Profiler to 64bit Storage Manager.

How come I only see Storage and/or Backup licenses in the Portal?
The licenses for other Profiler devices (Servers, Agents, Pollers, Virtualization, Fibre Channel Switches and Applications) have been rolled into the disks licenses. Although you still have to configure those devices, there is no longer a licensing step in the process. There are no more pollers for VMware - you can use as many agents as you need to monitor VMware.

Installing Storage Manager over an Existing Profiler Deployment

The STM5.0 installer will migrate your current Profiler server in place (all settings and history will be saved). Simply execute the installer on the Profiler server and it will find the current Profiler install and migrate the configuration and history.

Verify that your server has plenty of storage before you start (generally 2X the size of the Profiler directory). Once Storage Manager is installed, you can remotely upgrade your agents.

SolarWinds recommends backing up your database before you execute the Storage Manager installer. For more information on how to do this see Backing Up Your Database.

Clean Install of Storage Manager for Windows

The following section guides you through a clean install of SolarWinds STM for Windows. Installation steps for non-windows installations are located in the Storage Manager Administration Guide.

Before Installing:

- Close any services window(s). Installation will not work properly if you leave this window open during install
- **MySQL:** Uninstall any previous instances of MySQL. Only one instance of MySQL is supported at a time
- **Installation Path:** All STM binary and data files are located under the installation directory. When installing, select a directory located on a partition with enough space (we suggest 40 GB) to hold STM data files over time
- **Storage Manager** cannot be installed on the same server as **SolarWinds Virtualization Manager**

To install SolarWinds STM:

1. If you downloaded the product from the SolarWinds website, complete the following steps:
   a. Navigate to the location of your downloaded .zip file, and then extract the package to an appropriate location.
   b. Launch the SolarWinds STM Server executable.
2. Review the Welcome text, and then click **Next**.
3. Select setup type. **Express Install** is recommended for Evaluations.
4. Accept the terms of the license agreement, and then click **Next**.

   License: The built-in 30 day evaluation license will be used during install. After installing you will then enter your activation key.

   Path: The default install path will be: C:\Program Files\SolarWinds\Storage Manager Server\.

   Database Password: The default database password will be 'solarwinds'.

   STM Server will install these services:

   - **MySQL database:** the MySQL repository for all data collected by STM
   - **SolarWinds Storage Manager Collector:** collects data from agents
   - **SolarWinds Storage Manager Event Receiver**: receives traps
   - **SolarWinds Storage Manager Maintenance:** runs maintenance routines in the background
   - **SolarWinds Storage Manager Poller:** remotely polls devices or applications by a variety of methods
   - **SolarWinds Storage Manager Web Services:** the tomcat web server
5. Click **Finish** to exit the Setup Wizard.
6. Click the STM icon on your desktop or point your web browser at http://localhost:9000. You should see a Login Screen.

Note: The default Web Server Port can be changed in the server.xml file in the configuration folder `C:\Program Files\SolarWinds\Storage Manager Server\conf`. After changing, you need to bounce the Tomcat web service.

7. Login to the STM Server with the user name **Admin** and no password:

To complete the installation you will need to enter your product activation key that was previously copied.

Installing the Storage Manager Integration Module on your Orion Server

If you are using an Orion product (NPM, APM, etc…) with Core 2011.1 or later, you can install the Storage Manager Integration Module and see storage data inside of your Orion product.

To install the integration piece:

1. The integration module installer (`OrionIntegrationModuleforStorgaeManager.msi`) is included in the zip file you downloaded. Copy it to the Orion server (Core 2011.1 and later) and execute it.
2. **Go to Settings > Storage Manager Settings** and enter the IP address and login credentials you want to use. Note on some browsers, if you press the Test button, it will erase the password.
3. Click the **Storage** tab to see the Storage Manager main console.

Note: When you go from an evaluation license to a permanent license and are over your disk count, STM will unlicense arrays until the next array puts you under the licensed limit.

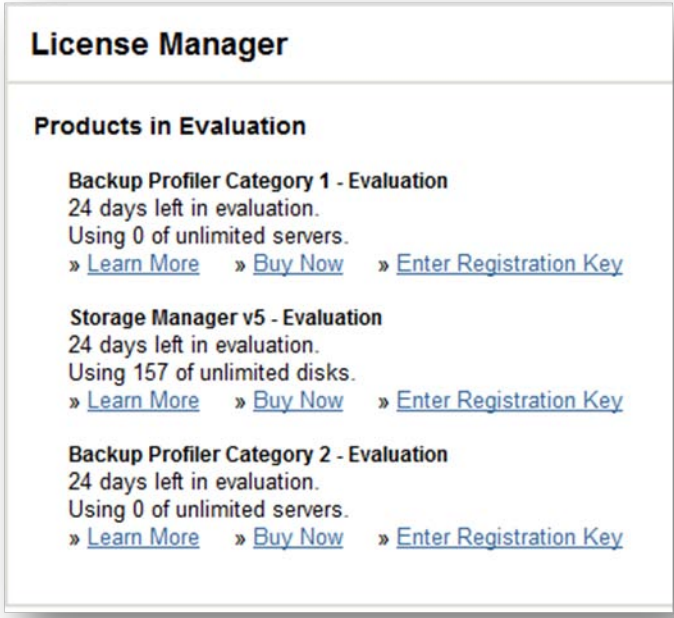
License Activation

After installing STM you will then need to activate the product using your registration key.

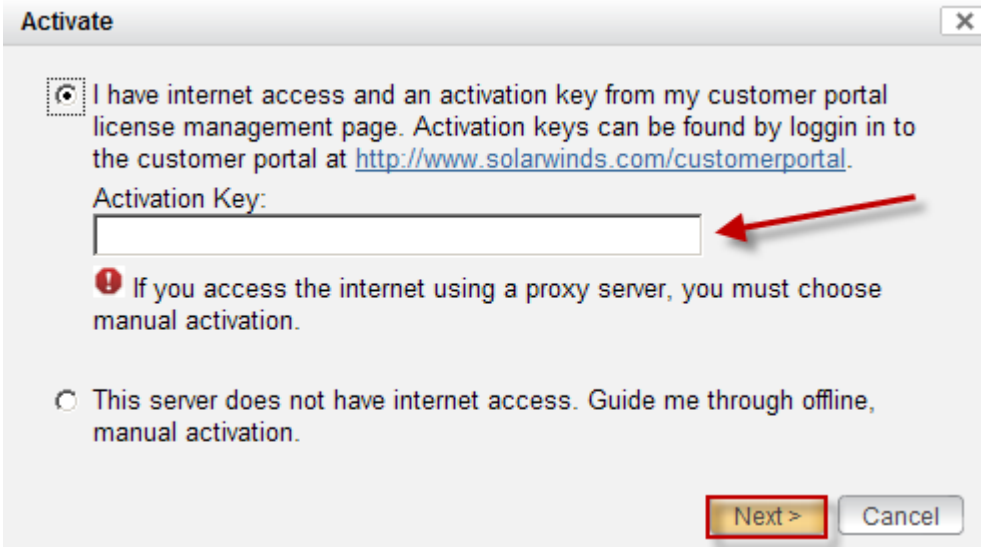
To activate your keys:

1. Login to the **Storage Manager** Web Console.
2. Click **Settings > License Manager**.

3. Click "**Enter Registration Key**" and then paste the string you copied from the customer portal. As long as the Storage Manager has internet access, it will activate the key and refresh the screen to show the newly activated key. If Storage Manager cannot reach the internet, there is a manual process to complete. Follow the onscreen instructions for offline activation.


License Manager
Products in Evaluation
Backup Profiler Category 1 - Evaluation
24 days left in evaluation.
Using 0 of unlimited servers.
» Learn More » Buy Now » Enter Registration Key
Storage Manager v5 - Evaluation
24 days left in evaluation.
Using 157 of unlimited disks.
» Learn More » Buy Now » Enter Registration Key
Backup Profiler Category 2 - Evaluation
24 days left in evaluation.
Using 0 of unlimited servers.
» Learn More » Buy Now » Enter Registration Key

4. Repeat the process for each key you want to activate (1 Storage and 2 Backup Categories).


Activate
I have internet access and an activation key from my customer portal license management page. Activation keys can be found by loggin in to the customer portal at http://www.solarwinds.com/customerportal.
Activation Key:
If you access the internet using a proxy server, you must choose manual activation.
This server does not have internet access. Guide me through offline, manual activation.
Next >
Cancel

5. Enter the Registration information and click **Register**.

License Manager Page

The License Manager page provides details about your main server license and any additional modules. This page also shows the service pack level which you are on.

To access this page:

1. Click **Settings > License Manager**.
    - **For example:** If you have a backup licensed you will see them listed as:

      Backup Tiers have two categories:

      Category 1: Backup Exec, Arcserve, Commvault

      Category 2: Legato, TSM, Netbackup

Installing Agents

The following steps detail how to upgrade your STM agents remotely This applies to all STM agents and later. If your agents are 4.11 or earlier, we have a separate upgrade utility

To install agents:

1. Verify the version of the agent in the Devices page.
2. ***If the agent version does not match the current version, then move on to upgrade the agent.***
3. Click **Settings > Updates & Upgrades.**
4. Click **Upgrade Agents.**
5. Provide a name for your Agent Upgrade activity. Select all the required modules and the Agents.
6. Click **Save** to push the changes.
7. Click **Module Push Report** for details on the Modules/Agents upgrade pushed.

Note: The Agent upgrade details are also available in Reports.

Under **Quick reports**, select **'Agent Upgrade History**' under '**Configuration**' and run the report.

http://knowledgebase.solarwinds.com/kb/questions/2393/Current+and+previous+Profiler+agent+downloads

You can download them for Windows, Linux, and Unix platforms and install them in a few minutes. Once installed, they will self-register with the Storage Manager server and automatically start monitoring the server they are installed on.

Manual Upgrade

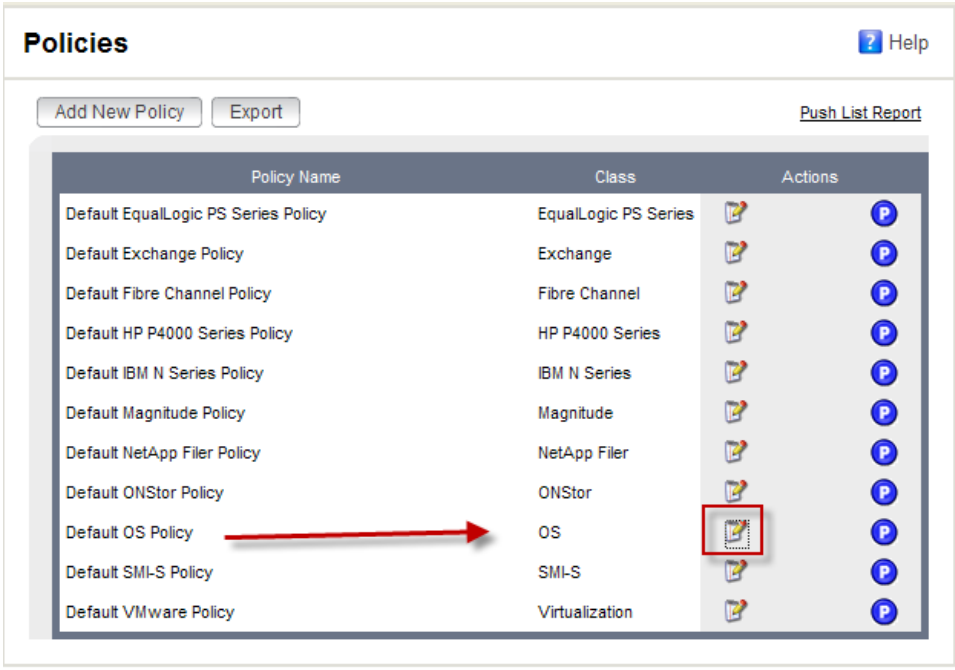
The above upgrade mechanism is done from the Server side. Agent Upgrades can also be done manually by executing the Agent build for that version on the Agent side itself. SolarWinds recommends upgrades to be done from the Server side to avoid data loss.

STM Agent OS Device Configuration

In most cases, an OS Agent will self-register with the STM server as a device. However, you can also define devices manually.

To change the default OS policy:

1. **Click > Settings > Policies > Default OS Policy**



2. Complete or change the following info:

a. Server IP Address: The Server IP Address of the server where the agent resides. Note: This is not configurable once the agent is created.

Device Display Name: The name you want to display for this device throughout STM.

HTTP Port : The port used by STM to collect data from the agent (default 4319). If you change this setting, STM will immediately try to connect to this agent and update its configuration. If STM is unsuccessful, then it will abort the changes. Otherwise, you might lose communication with the agent.

Active: The active agent. Uncheck this box if you want STM to stop collecting data from the agent. **Note:** Even though you make a Device inactive, the agent will continue to run and you will still receive traps and be able to configure the agent.

Device Groups: A device may be assigned to zero, one, or multiple groups. If you have any defined groups, the names of those groups will appear in the Available field.

- To assign a device to a group, simply click the group name in the **Available** field. The selected group name will automatically move to the **Selected** field.

- To remove a device from a group, simply click the group name in the **Selected** field and it will move to the **Available** field.

Note: ***If you save the device definition without assigning it to a group, then the device will appear as Unassigned in the Devices List.***

Monitor Agent: Check this box if you want the server to monitor the agent and send a trap if the agent has not been collected from. The inactivity threshold can be configured on the server setup page.

3. To save this device definition, click **Save**

STM Orion NPM Integration

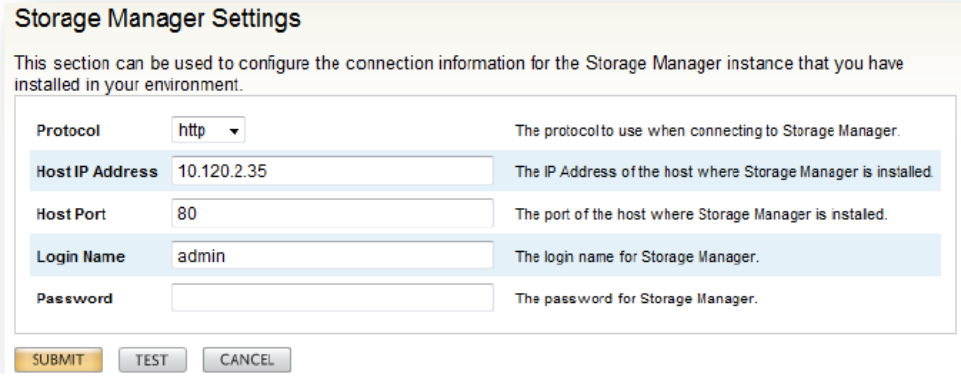
The STM download includes an integration module that can be installed on your Orion server. This light integration provides a Storage tab which can give you a quick view of your storage metrics.

Requires Orion core 2011.1 or later

To install the STM /Orion NPM integration piece:

1. Locate the integration module installer (***OrionIntegrationModuleforStorgaeManager.msi*)** that is included in the product download. Copy it to the Orion server (Core 2011.1 and later) and execute it.

2. Go to the **NPM Settings > Storage Manager** Settings and enter the IP address and login credentials you want to use.


Storage Manager Settings
This section can be used to configure the connection information for the Storage Manager instance that you have installed in your environment.
Protocol
http
The protocol to use when connecting to Storage Manager.
Host IP Address
10.120.2.35
The IP Address of the host where Storage Manager is installed.
Host Port
80
The port of the host where Storage Manager is instaled.
Login Name
admin
The login name for Storage Manager.
Password
The password for Storage Manager.
SUBMIT
TEST
CANCEL

Note: On some browsers, if you press the Test button, it will erase the password.

3. Click on the storage tab, to see the Storage Manager main console.

Note: When Storage Manager is configured to use LDAP authentication, then the domain is assumed by Storage Manager based on those settings. Therefore, when you configure the ***Orion Storage Manager Settings***, they should not specify the domain when filling in the ***Login Name*** field.

If you have configured LDAP authentication in Storage Manager, and configured a domain of ***foodev***, they will not include this in the ***Orion Storage Manager Settings*** page,

For Example: Instead of ***foodev\john.doe***, just use ***john.doe***.

The user can also configure the credentials for the ***admin*** user, as that user will be authenticated against the local Storage Manager user database, not LDAP, regardless of whether or not LDAP authentication is enabled.

Storage Manager Database

STM is bundled with its own database server. It uses MySQL® as its central data repository. This database server is very flexible, making database backup, external access (via ODBC) and handling very easy tasks. For more information regarding MySQL visit http://www.mysql.com.

Note: Using the STM MySQL server for applications other than STM can slow down performance and consume additional CPU devices.

MySQL Port:

STM runs MySQL database server on port 3306. SolarWinds strongly recommends not changing this setting. Contact http://www.solarwinds.com/support/ticket/ for assistance if you need to change it

Backing up the STM Database:

STM data backup and recovery are very simple processes. To backup your data:

1. Stop STM services.
2. Stop MySQL.
3. Make a copy of the entire data directory:
   a. The default path in Windows - C:\Program Files\SolarWinds\Storage Manager Server

Data Recovery:

In order to restore a backed-up database:

1. Stop STM services
2. Stop MySQL

3. Replace the data directory (see section above for paths) with the backed up directory
4. Restart MySQL
5. Restart STM services

MySQL Performance Tuning:

The MySQL Database Server should perform correctly under most situations and in most environments with the default configuration. If performance optimization is required, contact SolarWinds http://www.solarwinds.com/support/ticket/ for assistance on tuning MySQL.

Warning: If you have installed MySQL separately before installing STM Server, the install will be terminated as MySQL can support only one instance of MySQL at a time. Before installing, stop the MySQL Windows service (if any) and then uninstall MySQL. DO NOT manually delete any MySQL directories even after uninstall is completed! Old database data is located under the MySQL install directory.

Chapter 3

Web Console Navigation

The STM Web Console provides a consolidation of information about your enterprise.

The left navigation tree includes the following sections:

Event Monitor

The Event Monitor page summarizes the different events that are currently active (not cleared). Clicking the chart takes you to the Event Monitor screen.

Reports:

The SAN Group console aggregates information from both SAN devices and OS Devices that have file systems assigned to a SAN device. For example, in the image below, we have grouped a Xiotech Magnitude, a Brocade switch and five file systems together into a SAN group.

BackUpGroups:

The SAN Group console aggregates information from both SAN devices and OS Devices that have file systems assigned to a SAN device. For example, in the image below, we have grouped a Xiotech Magnitude, a Brocade switch and five file systems together into a SAN group.

Application Groups:

Server and NAS Groups:

- The SAN Group console aggregates information from both SAN devices and OS Devices that have file systems assigned to a SAN device. For example, in the image below, we have grouped a Xiotech Magnitude, a Brocade switch and five file systems together into a SAN group.
- The SAN Storage Status is an overview of the OS device file systems that have been mapped to the SAN.
- The SAN File System Trends and Forecast are the trends and forecast for the file systems that have been assigned to that SAN group.
- The SAN Status shows how the ports of each device are fairing and if they have any events.

Virtualization:

Settings: Provides quick access to all the STM settings.

Storage Summary Page:

Server Monitor

The Server Monitor page list the monitored servers and displays condition levels which are represented by various status icons.

Legend	
Status - Resource and Agent Status	
	Resource may have a problem
	There may be some issues with the resource
	Data collection issue
	No data available
	Resource is powered off
	Resource is normal
Disk | CPU | Mem | Net - Confidence Int.	
Note: The last known state is shown, even if the agent stops reporting data.	
	High Error Condition
	High Warning Condition
	Normal Condition
	Low Warning Condition
	Low Error Condition
	Unknown Condition
Off	Real time disabled for a parameter
N/A	Real time disabled
Vol - Drive/Volume Usage Threshold	
	At least one drive/volume exceeds usage threshold
	All drives/volumes below usage thresholds
Backup - Last Backup Status	
	Backup Failed
	Backup Successful (How long ago)
	Unknown Condition or Not Monitored

Backup Monitor

Backup Dashboard shows the status of the client groups based on the status of all clients in that group. We can also drill down each client group to view the status of all the clients in that group along with details like Group, Start Time, End Time, Backed Up MB. At a glance it provides, 8 days view of backup client group and client backup statuses.

SnapMirror Monitor

The SnapMirror Monitor shows the current transfer between the source and the destination for all the filers in the group or a particular filer based on the filter selection.

Getting Started Page

When you login to the web console you will see the **Getting Started with Storage Manager** section. This device provides quick access to adding storage devices to monitor. The left navigation menu provides access to all the remaining components of STM.

A summary of the **Getting Started Page** sections are as follows:

- Network Discovery

  Scan sections of your network to discover new devices to monitor.

- Servers

  Add servers to be monitored by STM. Follow the onscreen instructions for adding the OS agent.

- Virtualization

  Add VC Instances and stand alone VMware Hosts. Follow the onscreen configuration instructions.

- Storage Arrays

  Select the type of array to add and follow the onscreen instructions for configuration.

- FC Switches

  Select the type of fibre channel switches to add and follow the onscreen instructions for configuration.

- Backups

  Select the type of backup servers to add and follow the onscreen instructions for configuration.

Managing User Accounts

The User account function allows administrators to add, edit, and delete users from the STM application. Users' privileges are categorized into several levels, allowing administrators to create filtered views of information based on the user's responsibilities and need-to-know. These filters are created according to groupings of managed devices and devices. This function allows administrators to assign users to the appropriate group or groups of monitored systems for which they will be responsible.

Adding Users

Managing Existing Users

Adding Users

To add a new user:

1. Click **Settings > Manage Users**
2. Click **Add New User**
    a. Then enter the **Display Name**, and **Password**.

The password must be at least one character long; it is case sensitive. STM will require you to retype the password again in the **Confirm Password** field.

3. Click **Save.**

There are several user account options to choose from.

- Root administrator
- Read Only Administrator- User has read- access only
- Group Administrator- User access is defined by the root administrator
- User – User access is defined by the root administrator
- Backup Monitor only

Select the levels of user privileges:

Login

Users with login privileges can access event screens as well as device inventory usage and performance reports for all devices in their assigned groups.

To grant login privileges, check the Login screen. To indicate which device information the User is allowed to access, highlight the desired device group(s) in the column entitled Available and click to move the desired group(s) to the Selected column.

Once the groups are selected, click Add to activate the privilege. The user will then have access to those defined group(s). For example, if only the NT Group was selected, then the user would only be able to access Event Lists, Event Histories, Usage Reports and other information about Windows NT systems assigned to the NT group.

Users with login privileges can access the STM application, but the view of the STM main menu will be filtered. For example, login users will not see the Administration portion of the menu that contains folders for defining Groups, Devices, Server Setup and Users.

In addition, STM allows you to select the type of data a user can see.

- Backup - Backup Servers and Clients
- Device - All DAS and NAS devices
- SAN - All SAN devices (Fibre Channel and EMC)
- Application - Application devices
- Storage Group - Logical groupings of File systems
- Management Reports - Can run management reports

Administrator

Administrators can see all data about all devices in all groups. Administrators also have access to all STM menus, screens and reports, including the Administration menu. To grant administrator privileges to a user, check the Administrator field and then click **Add**.

Editing User Profiles

To edit a user:

To access the User accounts:

1. Click on **Settings**
2. Click on **Users**

1. Click the edit icon in the row where that user's name appears on the Users screen. The User's Profile screen is displayed.
2. To edit any User Info fields, click the Edit icon in the User Info frame.
   a. If you edit the password, STM will require you to retype the password again in the Confirm Password field.
3. To change user privileges, check /uncheck the Login and/or Administrator boxes.
4. To edit email addresses and/or notifications, return to the Profile page. (The Profile page can also be reached by clicking on the Users option in the drop-down menu that appears under the Settings folder of the STM main menu at the left side of the screen, and then clicking on the Edit icon in the row of the user you wish to edit.)

5. You may edit the email address of the user or add new email addresses. Multiple email addresses and aliases can be entered if necessary. Entered email addresses will receive notifications from all devices specified in the Notifications field.
6. To modify the list of devices that will send alert notifications to a user, click on the Edit icon in the Notifications frame.
7. Click on the drop-down menu for Choose a Type to select either a group of devices or a specific device to be added to the notifications list. You may also choose the severity of Notifications to be sent: critical, error, warning, information and debug.

Discovering and Adding Devices

This section details the process of discovering network devices and then adding them to the STM database. There are two ways to accomplish this—Network Discovery by simply entering an IP address range to scan and by adding devices individually one at a time.

The method recommended largely depends on the number of devices added. To discover and add a larger number of devices across your enterprise, the Network Discovery is available. This chapter provides instructions for quickly populating your STM database with the network devices.

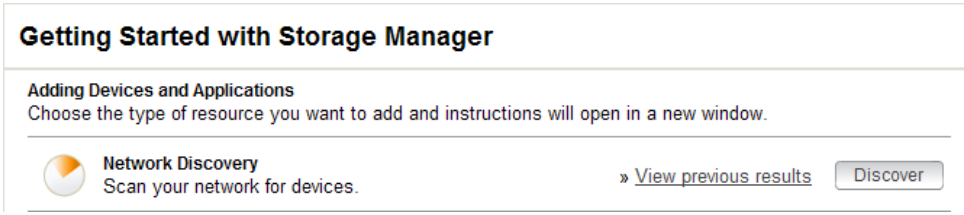
- Network Discovery
- Adding and Editing Devices
- Editing Devices
- Activating/Deactivating Polling
- Deleting Devices

Network Discovery

The STM Discovery feature quickly scans for EMC, LSI (IBM 3/4/5 series, Dell MD3xxx series, and SUN 2K/6K series), NetApp Filers, VMware vCenter and Standalone ESX arrays.

When new arrays or hosts are discovered, STM displays the hostname and IP Addresses so you can easily assign them to the management server to be configured.

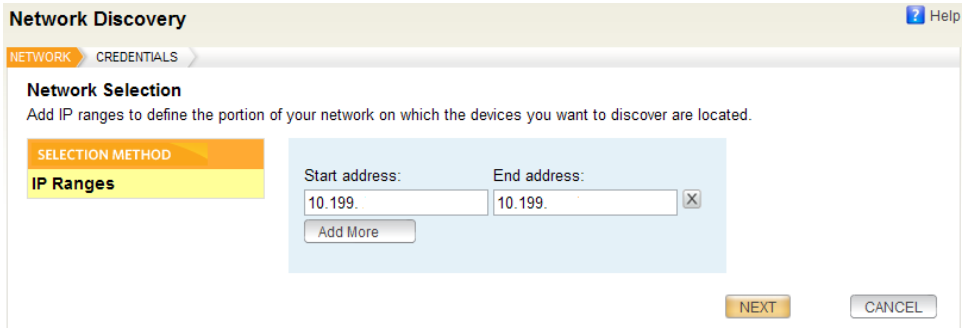
Note: For EMC and LSI based arrays, your SMI-S provider must be installed and configured for discovery to work.


Getting Started with Storage Manager
Adding Devices and Applications
Choose the type of resource you want to add and instructions will open in a new window.
Network Discovery
Scan your network for devices.
» View previous results
Discover

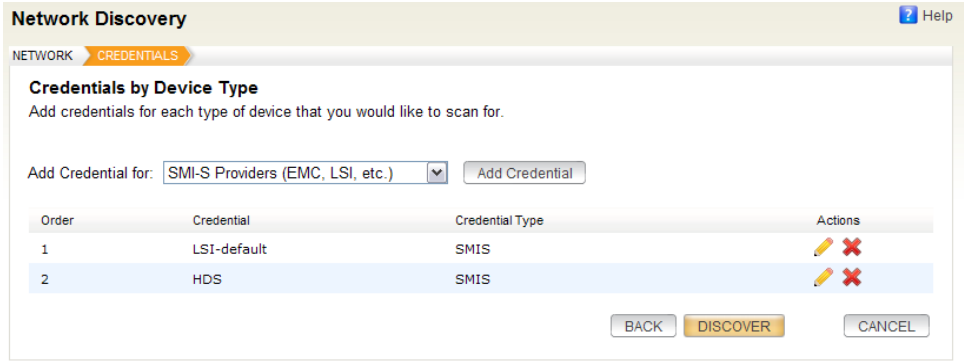
The Getting Started page allows you to add devices at any time.

To begin Network Discovery

1. Click **Discover**
2. Add IP ranges to define the section of network for the discovery scan



3. Click **Next**
4. Add the necessary credentials for each type of device to be scanned.



5. Click **Discover**
6. Click **Next** to assign the discovered devices
7. Select each device by check mark and then click **Assign to Agent**

(Assign VC, Assign ESX, Assign Array)

Note: When VC is assigned it will do an additional discovery in which additional ESX servers discovered will need to be configured on the **Getting Started Page.**

a. Select from the dropdown

b. Click **Save**

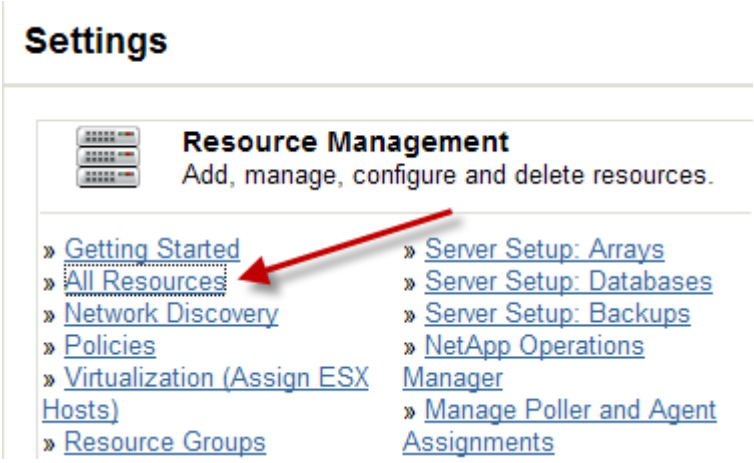
Editing Devices

The **All Devices** section allows you to add and edit applications and devices or edit existing devices.

Devices are the storage devices that you want to monitor.

To define, modify, or delete a device:

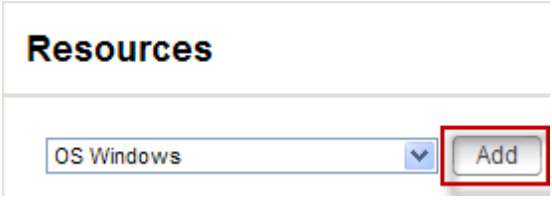
1. Click the **Settings** link under the left tree navigation.
2. Click **All Devices.**



The **All Devices** page displays a listing of all devices currently defined in STM.

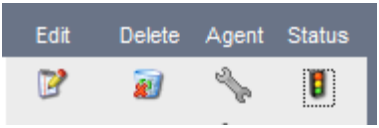
There are several actions you can take on this page.

You can add a device directly by selecting the desired device and clicking **Add.**



After entering the necessary information, the device will appear in the device list for management

Clicking the icons below allows you to edit, delete, configure Agents, and verify the current status for the selected device.



Editing Devices

To edit the information about a device, click the edit icon (pencil/paper) in the same row as the device's name. The screen that is then displayed contains the current information about that specific IP Device, including IP address, device name, SNMP Port, Trap Port, Community String, Group, and Agent Licenses, and whether the IP device is Active or not.

To edit the Device:

1. Click the **Edit** icon.
2. Enter new information in the desired fields.
3. Click **Save**.

To change the IP Address for any agents:

1. Set the self register option as **'no'** in Server setup page.
2. Change the IP Address in the Agent.
3. Change the IP Address in STM server.
4. Set the self register option as **'yes'** in Server setup page.

Activating/Deactivating Polling

Important: From the Edit screen verify that the **Active** checkbox is checked.

For STM to poll and collect data from a device; the **Active** checkbox should be checked. Similarly, to stop STM from collecting or polling data from a device, uncheck the active box. The change will take effect at the next scheduled collection time.

Note: Even when a device is marked inactive, you can still change the agent's configuration, the agent will continue to send traps, and you can still view data about that device.

Deleting Device

To delete a device from STM, return to the device screen and click the trash can icon. A dialog box will appear requesting confirmation.

Agent Status

Agent Status displays the status of the modules installed on the client. When you click the **Status** icon, an Agent Status window will appear.

Data Retention Policies

Data Retention Policies allow Administrators to define the duration that they wish to keep each kind of data. The policies are executed once every twenty-four hours by the STM Collector service. Data Retention Policies are divided into the following categories:

- Backup
- Database
- Events
- Operating Systems
- SMI-S
- SNMP/FC/HBA
- System
- Virtualization

These categories are subdivided into types of data. Each type of data may have a retention policy for raw and hourly data.

When the Data Retention Policy is enforced once a day, old data will be removed from the database.

For example: You have configured Operating **Systems > Disk Usage > Raw Data** for "**3 months**." When this policy is enforced, ALL disk usage data for ALL devices older than 3 months will be deleted.

If you select **Forever**, data will never be deleted

Chapter 4

Server Setup

Define the parameters of your Storage Manager server. These parameters are separated into the following functions:

- Agent Settings
- Array Settings
- Backup Settings
- Database Settings
- Email Settings
- File Analysis Settings
- GUI Settings
- Real Time Settings
- Reporter Settings
- Server Settings
- Trap Forwarding SettingsTrap Forwarding Settings
- User Authentication Settings (LDAP Authentication)
- Virtualization Settings

The following steps detail the parameters for your Sever Setup.

To access the Server Setup function:

1. Click **Settings > Server Setup All**.

Agent Settings

The Agent Settings define the behavior of the STM server when it receives a registration trap from an agent trying to register. Enabling these allows you to receive real time alerts when an agent status changes from yellow to red or from green to yellow. This will send out a trap.

- **Allow Self-Register** defines what STM does when it receives a trap from an agent that is not in the devices table. If set to true, STM adds the agent to the device table, using the IP address as the device name. Default is yes.

- **Auto Assign OS License** determines if STM automatically assigns an OS RTU License when it registers an agent. Default is yes.
- **Agent Inactivity Threshold** Choose the threshold for agent inactivity. If there has been no collection from an agent for the period specified, then an 'Agent not collecting' trap is sent. This trap is only sent for the agents to which the monitor agent check box is selected in the edit page.
- **Agent Status Alert** sets Alert status to TRUE/FALSE. Any change made to this parameter should be followed by the restart of the STM Event Receiver service.
- **Always alert when Agent status is Critical or Warning** sets status to TRUE/FALSE. The 'Agent Status Alert' parameter should be set to 'TRUE'.
- **Agent Status Alert Frequency** sets Alert Frequncey levels. Default is five minutes. The 'Agent Status Alert' parameter should be set to 'TRUE'. Any change made to this parameter should be followed by the restart of the STM Event Receiver Service.

Array Settings

The Array Settings control the behavior of the NAS and the Xiotech Magnitude poller.

- **EMC Celerra TCP Dump Interval** sets the TCP dump capture period.
- **EMC Celerra TCP Dump Frequency** sets the TCP dump capture frequency.
- **NetApp Include Snapshot** select YES / NO.
- **Xiotech Asset Frequency** sets the frequency that asset and allocation information is polled.
- **Xiotech Performance Frequency** sets the frequency at which performance information is gathered.
- **C-Level Data Collection Frequency** sets the frequency to Daily / Always / Never.

Backup Settings

The Backup Settings allow the administrator to set parameters involved in backup.

- **Backup Window Start Time** specifies the beginning of the Backup Window and the Backup Cycle (24-hour period). STM uses the backup cycle to summarize backup data, so it is very important that you define this parameter to mirror your actual environment closely.
- **Backup Window End Time** specifies the end of the backup window.

- **NetBackup: Treat job exit code 1 as** lets the administrator determine whether or not an exit code 1 should be logged as a success or failure.
- **NetBackup: Treat job exit code 71 as** lets the administrator determine whether or not an exit code 71 should be logged as a success or failure.
- **Backup Server Inactivity Threshold** sets the inactivity threshold for backup servers.
- **Automatic Client Mapping** turns on Auto Client Mapping to match incoming client data to devices already present in ${applicationScope.productName}.
- **NetBackup: Show only final status of client** setting the status to "yes" will set the final client status to that of the last job executed for the client-policy combination in the backup cycle.
- **Legato: Show Inactive Clients** Show legato inactive clients every cycle. By default it is turned off.
- **Percent Change Increase Threshold Color Coding** sets the color coding thresholds for Percent Change in Client Monthly Change report. Enter "5,10,20" to show 0 to 5% as Green, 5 to 10% as Yellow, 10 to 20% as Orange and greater than 20% as Red. You can enter from one to three threshold values. Enter "off" to turn off this feature.
- **Percent Change Decrease Threshold Color Coding** sets the color coding thresholds for Percent Change in Client Monthly Change report. Enter "-5,-10,-20" to show 0 to (-5)% as Green, (-5) to (-10)% as Yellow, (-10) to (-20)% as Orange and greater than (-20)% as Red. You can enter from one to three threshold values. Enter "off" to turn off this feature.
- **Enable Backup Clients auto grouping** may be changed to No / Auto Group clients into server group / Use Regular expression to auto group clients, according to the need.
- **Auto Group RegEx pattern (e.g) Pattern "([^-]+)-" creates Group "tek" from the client "tek-nbu"** list of patterns that can used in group creation.
- **Enable Device Discovery** may be changed to enable/disable the device discovery feature. When enabled you will find a new option under Settings called "Device Discovery Config". The IP address range you wish to monitor should be entered in the "Include" section. Save the changes (YES or NO) to the "Device Discovery Config" page and restart the ${applicationScope.productName}WebServer service. STMwill scan the network for all IP addresses specified in the "Include" range on a regular 12 hour schedule.

- **NetBackup:Exclude Exit Codes from Final Status summary Reports** This parameter will exclude all the exit codes added in this option from the NetBackup Final Status Summary report.
  Valid IP addresses will be used to generate a list of Legato, TSM and NetBackup clients which are not being backed up by those servers respectively. The reports can be located under the "Reports" section for the specific backup server type. To turn off this feature select "no" and restart the Web Server.

Database Settings

The Database Settings control the behavior of the Oracle and the SQL-Server Poller.

- **Oracle Performance Polling Frequency** allows administrators to specify how often STM gathers performance data from server-attached Oracle RDBMS.
- **Oracle Usage Polling Frequency** allows administrators to specify how often STM gathers usage data from server-attached Oracle RDBMS.
- **SQL Server Performance Polling Frequency** allows administrators to specify how often STM gathers performance data from server-attached SQL Server RDBMSs.
- **SQL Server Usage Polling Frequency** allows administrators to specify how often STM gathers usage data from server-attached SQL Server RDBMSs.
- **SQL Server Table Fragmentation Hour** sets the start time to run the DBCC ms-sql command to collect table fragmentation stats.

Email Settings

- **Email Server and Email From** specifies the email account that STM will use to send email notifications and reports. The defaults should be changed immediately.
- **Email Server Port:** Specify the port to be used for e-mail systems that requires authentication. When using secure SMTPS protocol.
- **Email Server Username & Email Server Password:** Provide valid Username and Password for e-mail systems that requires authentication. For example: When using secure SMTPS protocol.
- **Use SMTPS:** Select 'Yes' if using e-mail systems that requires authentication. Else select 'No'.

File Analysis Settings

All settings that control the behavior of file analysis and data classification.

- **File Age Categories** sets the coding thresholds for File Age reporting values in reports.
- **Always Pre-Select All NAS Shares** determines if all shares are selected to be available to assignment to an agent automatically (Yes) or if you have to manually select the shares before you can assign them to an agent (No).
- **Ungrouped File Type Details** determines whether to store detailed information on ungrouped file types in database.

GUI Settings

All settings that control how the GUI behaves at the enterprise level.

- **Server Monitor Refresh Frequency** sets the frequency at which you want to refresh the Server monitor.
- **Max Data Points for Storage Trending and Forecasting** sets the maximum number of data points that STM will trend for storage usage. For example, 30 means STM will go back 30 days (assuming one point per day) while doing analysis. The minimum is 15 points.
- **Server Monitor Filter** filters the list of Servers in the Server Monitor and Server Status bar by last collect time.
- **Enable IPAddress Change** allows the IP addresses of servers to be changed on the Device Page.
- **Enable Storage -Share Group Assignment by filter only** Select this feature to enable storage share group assignment using only the filter. Enable this option when there are a large number of shares.
- **Track invalid log in attempts in Window Event Log** Select true if you want to track any invalid log in attempts in the Windows Event Log. This is applicable only for Server installed on Windows OS.
- **Email Notifications for SNMP Alerts** Select 'First Occurrence' to receive an email notification 'once' for the first time when a trap comes in (or) select 'Every Occurrence' to receive an email notification 'for every repeated occurrence of the trap. In case of iservice, this sends out an email notification every minute, whenever the iservice is down.

Real Time Settings

Each of the following parameters allows the user to set the minimum threshold for the HIGH warning and error conditions evaluated by the Real-Time confidence intervals.

For example: If the confidence interval evaluates CPU Busy on a server to 12% for warning and 33% for error, STM will adjust those settings higher to meet the minimums set here (15% and 40% respectively).

- **CPU Error Minimum** sets the minimum CPU Busy for a HIGH Error threshold.
- **CPU Warning Minimum** sets the minimum CPU Busy for a HIGH Warning threshold.
- **Disk Error Minimum** sets the minimum Disk I/O for a HIGH Error threshold.
- **Disk Warning Minimum** sets the minimum Disk I/O for a HIGH Warning threshold.
- **Memory Error Minimum** sets the minimum Memory for a HIGH Error threshold.
- **Memory Warning Minimum** sets the minimum Memory for a HIGH Warning threshold.
- **Network Error Minimum** sets the minimum Network I/O for a HIGH Error threshold.
- **Network Warning Minimum** sets the minimum Network I/O for a HIGH Warning threshold.

Reporter Settings

The Reporter settings allow administrators to specify Server parameters.

- **Maximum Report Rows** sets the maximum number of rows a report is allowed. When you run a report, you can also specify the number of rows you want to display.
- **Delete Published files Older Than** sets the number of hours or days that published reports are retained.
- **Date Format** sets the way dates will be displayed in reports and consoles.
- **Report Charset** sets charset encoding for reports.
- **Percent Usage Color Coding** sets the color coding thresholds for Percent Usage values in reports and on Device Consoles. Enter "70,80,90" to show 0-70% as Green, 70-80% as Yellow, 80-90% as Orange and 90-100% as Red. You can enter from one to three threshold values. Enter "off" to turn off this feature.
- **Server Name** sets the name of the Server
- **Server Port** sets the port of the Server

Server Settings

The Server settings control the overall behavior of the collector, the SNMP and DNS Poller, how the server sends email, and the global configuration of File Age Categories.

- **Delete Log files Older Than** sets the duration server log files are retained on the server.
- **Delete Output files Older Than** sets the duration temporary files are retained on the server.
- **SNMP Trap Port** sets the port you want to receive traps on. **Note:** If you change this setting, you should restart the event receiver.
- **Data Retention policy Start Time** sets the time you want Data Retention policies to be executed. Data Retention Policies can tax a system for a short period because every table is analyzed. It is recommended that you run this analysis when the machine is not busy.
- **Hosts Down Monitor Enable** default is YES. If set to NO, then the functionality of 'Host Not Responding to Ping' trap is disabled. Any change to this parameter either (YES / NO) should be followed by the restart of the STM Event Receiver service.
- **Web Server Log Level** sets the level of STM Reporter Web Server log messages.
- **Maintenance Log Level** sets the level of STM Reporter Maintenance log messages.
- **Poller Log Level** sets the level of STM Reporter Poller log messages.
- **Event Receiver Log Level** sets the level of STM Reporter Event Receiver log messages.
- **Collector Performance Monitor** turns Collector Performance Monitoring on or off.
- **SNMP Table Poll Timeout** sets maximum time allowed for polling an SNMP table.
- **Automatic Clearing of Traps Frequency** sets frequency to clear traps older than trap age threshold.
- **Automatic Clearing of Traps Age** sets the trap age threshold for automatic trap clearing.
- **DNS Polling Frequency** sets the frequency at which the DNS Poller will poll the DNS agents you have defined.
- **Chart Image Format** sets the chart image format to either PNG or JPG default format is PNG.

- **Collector Frequency** allows administrators to specify the maximum time between collection attempts, ranging from 30 minutes to daily. Every 15 minutes, STM checks every device and if the time since the last successful data collection is greater than the time specified in this field, the server adds the device to the collection list and attempts to collect data from the agent on that device.
- **SNMP Frequency** sets the interval (30 min. to daily) the server uses for SNMP-standard GET commands to collect MIB II data from SNMP-enabled monitored devices.

Note on SNMP traps: The STM Event Receiver continues to receive SNMP traps as they arrive regardless of the setting in this field.

Trap Forwarding Settings

The STM server and its agents can generate traps that are sent to the STM Trap Receiver. To forward these STM traps to a network operations center, configure the trap forwarding features of STM

STM only forwards STM traps currently.

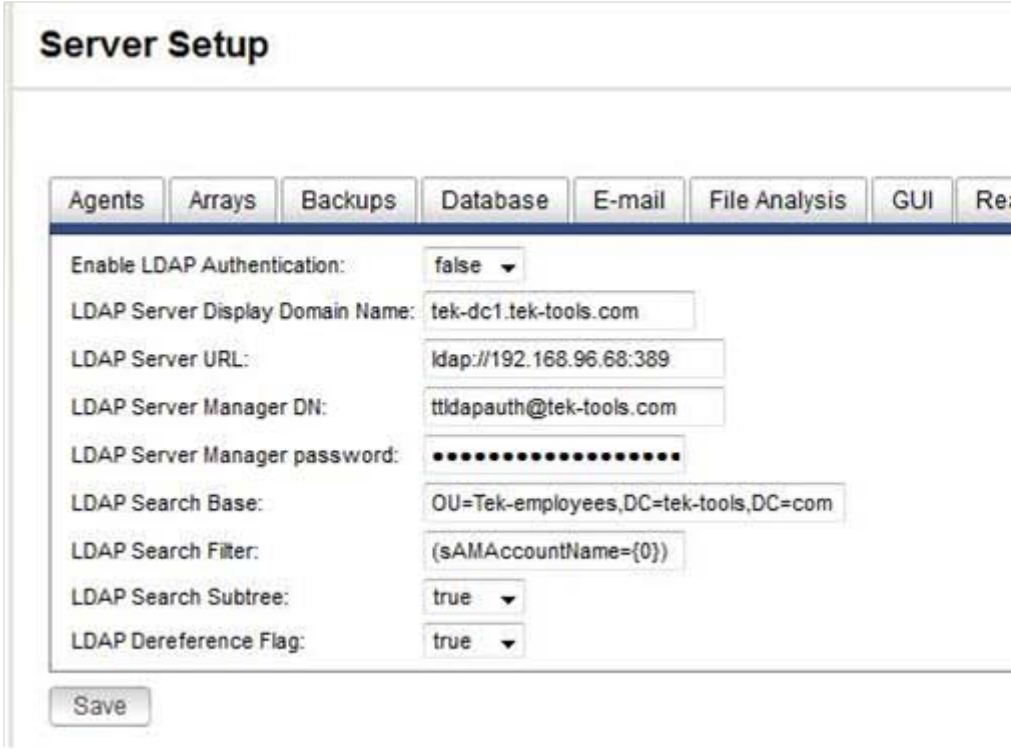
- **Forward $ STM Traps** enables the forwarding of traps when set to true.
- **Destination IP** sets the IP address of the server to which you want to forward traps.
- **Destination Port** sets the port of the server to which you want to forward traps.
- **Community String** sets the community string of the server to which you want to forward traps.
- **Disk Usage Warning Limit** sets the threshold for a file system, volume or drive that you want to forward as a Warning trap.
- **Disk Usage Critical Limit** sets the threshold for a file system, volume or drive that you want to forward as a Critical trap.
- **Disk Usage Error Limit** sets the threshold for a file system, volume or drive that you want to forward as an Error trap.
- In general, you want the Warning Limit to be less than the Critical Limit, which will be less than the Error Limit (ex., 70 < 80 < 90).
- **Persist Trap** determines if trap is persisted in database.

User Authentication Settings (LDAP Settings)

- **Enable LDAP Authentication** Enables LDAP Authentication when set to True

- **LDAP Server Display Domain name** Provide display name for LDAP server
- **LDAP Server URL** Provide URL for LDAP Server
- **LDAP Server Manager DN** Provide Domain Name for LDAP Server Manager
- **LDAP Server Manager password** Provide password for LDAP Server Manager
- **LDAP Search Base** Specify LDAP search base
- **LDAP Search Filter** Specify LDAP filter
- **LDAP Search Subtree** Searches LDAP subtree when set to True
- **LDAP Dereference Flag** LDAP Server performs dereferencing when set to True

For example:



Virtualization Settings

- **VM Age Categories by Boot Time** sets the coding thresholds for VM Age Categories by Boot Time reporting values in reports.
- **Capacity Forecasting Target Utilization** sets the utilization range from 50% to 100%
- **CPU Distribution Category** specifies as many categories needed, but the alignment may not look proper in the chart if the count goes more than 7. 1,2,3,4 will lead to 5 categories in the pie chart with (1CPU,2CPU,3CPU,4CPU,Other) colors .
- **Memory Distribution Category (MB)** similar to the CPU Distribution Category, but values need to be specified in MB.
- **Storage Distribution Category (GB)** similar to the CPU and Memory categories, but the values are matched based on the range; If you specify 10,20,30,40 in the charts there will be 5 categories as 0-10,10-20,20-30,30-40 & > 40 GB
- **Heatmap Percentage Category** specifies two values for specifying the Heatmap range. 10,50 will manipulate to 0-10 as cold,10-50 as warm and >50 as hot

Note: The following are the parameters which require a restart of some of the STM Services for the effect to take place. For all others, the Services do not need to be restarted, but they will take into effect only going forward. No changes will be done to historical data.

Server Setup Parameter - Function	**Name of the parameter**	**Name of the service to be restarted**
Backups	Enable Device Discovery	SolarWinds Storage Manager Web Services
Server	Agent Status Alert	SolarWinds Storage Manager Event Receiver
Server	Agent Status Alert Frequency	SolarWinds Storage Manager Event Receiver
Server	Agent Status Alert Frequency	SolarWinds Storage Manager Event Receiver

Chapter 5

Monitoring Storage Arrays

STM monitors arrays in a variety of ways – SMI-S, SNMP, API, Telnet/SSH, and each method can have extra requirements to enable discovery and monitoring.

Here is a summary of how each supported array is monitored and if there are extra requirements:

Device	Method	Additional Software required
3PAR	SMI-S	No, SMI-S built into the array.
Dell Compellent	SMI-S	No, SMI-S built into the array
Dell Equalogic	SNMP	No.
Dell MD3xxx	SMI-S	Yes, download and install the LSI SMI-S Provider.
EMC Celerra	Telnet/SSH	
EMC Clariion, VNX	SMI-S	Yes, download and install the EMC SMI-S Provider.
EMC Symmetrix, DMX, VMAX	SMI-S	Yes, download and install the EMC SMI-S Provider.
HDS	SMI-S	No, packaged in XXX.
HP EVA	SMI-S	No, packaged in XXX.
HP P4000	SNMP	No.
HP XP	SMI-S	No, packaged in XXX (same as HDS).
IBM DS3xxx, DS4xxx & DS5xxx	SMI-S	Yes, download and install the LSI SMI-S Provider.
IBM DS6xxx, DS8xxx	SMI-S	No, SMI-S built into the array.
IBM ESS -	SMI-S	Yes, download and install the SMI-S provider.
IBM N-Series	API	No.
IBM SVC	SMI-S	No, SMI-S built into the array.
LSI	SMI-S	Yes, download and install the LSI SMI-S Provider.
NetApp Filer	API	No.
NetApp Operations Manager	API	No.
ONStor	SNMP	No.
Pillar	SMI-S	No, SMI-S built into the array.
Sun StorageTek 2xxx, 6xxx & FLX Series	SMI-S	Yes, download and install the LSI SMI-S Provider.
Sun StorageTek 99xx Series	SMI-S	No, packaged in XXX (same as HDS).

Xiotech 3D 4000 and Emprise	Web Services	No

Storage Array Requirments

The follwing is a list of requirements needed to monitor your devices using STM.

Select the vendor:

- 3PAR
- Dell EqualLogic
- EMC CLARiiON Series
- EMC Celerra
- HP EVA
- HP P Series (Lefthand)
- IBM DS 3K, 4K, 5K
- IBM DS 6K, 8K
- IBM SVC, V7000
- LSI
- NetApp
- SUN/StorageTek

3PAR	
Versions/Models	All F Class and T Class InForm OS 2.3.1 and higher
Features	Asset Storage Performance
Requires Agent?	No agent installed on array
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• IP Address of the 3PAR storage array • SMI-S provider is embedded on the storage array. The provider must be started prior to connecting to it. Login to the CLI on the array and run “startcim”. • Type: “showcim” to confirm Inform OS version • Identifier– Type:”showport”, Node_wwn is the identifier • Username and Password to the array
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write	Read Only

Actions	
Ports Used	Configurable: 5988 (HTTP) or 5989 (HTTPS) used by 3PAR provider.
Communication	• See the STM Ports section below. Can be HTTP/HTTPS between proxy agent and 3PAR SMI-S provider.
Installation	• Configuring a 3PAR device
EMC Celerra	
Versions/Models	NS Series
Features	Asset Storage Performance VDMs Data Classification (File Analysis)
Requires Agent?	No
Requires a Proxy Agent?	Yes – via Profiler Server
Prerequisites	• nasadmin login or equivalent • Same login for all Control Stations; passwords can be different • SSH connectivity between Profiler Server and EMC Control Station
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	Non-Configurable: 22 on the Control station
Communication	SSH between Profiler Server and each EMC Control Station
Data Classification	• Occurs via Proxy agent. • CIFS Shares require a Profiler Windows Agent and domain account to access the shares being analyzed • NFS Shares require a Profiler UNIX Agent and root access to shares being analyzed.
NetApp	
Versions/Models	All
Features	Asset Storage Performance
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• IP Address of NetApp head/cluster node • Define user account on NetApp. Minimum access - a role with access to execute specific API calls. List

	available upon request. Usually provided just the root login • Add Proxy agent to list of trusted hosts on the NetApp storage system • ONTAP 7.3.x: Turn off API XML validation on each filer (FAQ-132)
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	• 80 (HTTP)/443 (HTTPS) on NetApp head/cluster node • Any available for CIFS/NFS
Communication	• See the STM Ports section below. • Can be HTTP/HTTPS between proxy agent and the NetApp head/cluster node
Data Classification	• Occurs via Proxy agent. • CIFS Shares require a Profiler Windows Agent and domain account to access the shares being analyzed • NFS Shares require a Profiler UNIX Agent and root access to shares being analyzed.
Dell EqualLogic	
Versions/Models	4.x
Features	Asset Storage Performance
Requires Agent?	No agent installed on array.
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• IP Address of the storage array • Read-only SNMP version 1 community string for the EqualLogic group
Credentials	• UNIX - Run as root • Windows - Local System account/Domain Account
Read/Write Actions	Read Only
Ports Used	161 (UDP) on the EqualLogic Group IP
Communication	See the STM Ports section below.
EMC CLARiiON Series	
Versions/Models	All
Features	Asset Storage Performance
Requires Agent?	No agent installed on array.
Requires a Proxy Agent?	Yes – Windows or UNIX

Prerequisites	• IP Addresses of Controller A (SPA) and Controller B (SPB) • Identify firmware/Flare code of array and confirm it is compatible with latest SMI-S provider. *Some older firmware is only compatible with older SMI-S provider versions. • If the array has Flare Code 26 it requires EMC SMIKit 6.4.2 (Provider 3.2.2) and higher • Install EMC Solutions Enabler with SMI-S on a Windows/Linux server with IP connectivity to the array controllers. • User account on Navisphere with admin/manager privileges on the CX array • For each CX, enable "Statistics Logging" for all storage processors via Navisphere • If SMI-S provider is on a server connected to the SAN being monitored see FAQ-92. • Note: CX600 arrays – require a Flare code higher than 16 (2.16.x.x.x) for data to be gathered using SMI-S
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	• Configurable: 5988 (HTTP) or 5989 (HTTPS) used by EMC Solutions Enabler • Non-configurable: TCP Port 443 bi-direction between provider and Clariion.
Communication	• See the STM Ports section below. • Can be HTTP/HTTPS between proxy agent and EMC Solutions Enabler
HP EVA	
Versions/Models	4000, 5000, 6000, 8000
Features	Asset Storage Performance
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• CommandView 8.02 with SMI-S CIMOM installed is recommended by HP, but CommandView 7.x will provide asset and storage info. • EVA8000 requires CommandView 8.0.2 and Firmware 6200 for Profiler to be able to show array Performance.

	• CommandView ID and Password for the provider. • Define user account on Command View EVA managing EVAs. Local user for CV-EVA v7.x; Domain/Local user for CV-EVA v8.x
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	Configurable: 5988 (HTTP) or 5989 (HTTPS) used by HP CommandView
Communication	• See the STM Ports section below. • Can be HTTP/HTTPS between proxy agent and HP CommandView
HP P Series (LeftHand)	
Versions/Models	P4000
Features	Asset Configuration Storage
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows, Linux, or Unix
Prerequisites	• SNMP enabled • Proxy agent in Access Control list • IP address of management node and each node
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	161 on management node and each node
Communication	• See the STM Ports section below. • SNMP from Proxy agent to management node and each node
IBM DS 3K, 4K, 5K	
Versions/Models	3000, 4000, 5000
Features	Asset Storage Performance - Disk Performance
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• IP Address of Storage Processors • Latest LSI Engenio SMI-S Provider installed on a 32 bit Windows/UNIX server that has IP connectivity to the storage processors

Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider Non-Configurable: 2463 used to set RPC sessions to the storage controller from SMI-S provider.
Communication	• See the STM Ports section below.. • Can be HTTP/HTTPS between proxy agent and the LSI Engenio SMI-S provider.
IBM DS 6K, 8K	
Versions/Models	6000, 8000
Features	Asset Storage Performance
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• IP Address of the Storage Manager • ID and Password to Storage Manager • Latest IBM SMI-S Provider installed on a Windows/UNIX server that has IP connectivity to the Storage Manager server. Can also monitor these via the HMC. Needs to be enabled via IBM.
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider
Communication	• See the STM Ports section below. • Can be HTTP/HTTPS between proxy agent and the IBM SMI-S provider.
IBM SVC , V7000	
Versions/Models	SVC
Features	Asset Storage
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• IP Address of IBM SVC • Latest IBM SMI-S Provider installed on a

	Windows/UNIX server that has IP connectivity to SVC
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider
Communication	• See the STM Ports section below. • Can be HTTP/HTTPS between proxy agent and the IBM SMI-S provider.
LSI	
Versions/Models	All
Features	Asset Storage Performance Disk Performance
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• IP Address of Storage Processors • Latest LSI Engenio SMI-S Provider installed on a 32 bit Windows/UNIX server that has IP connectivity to the storage processors
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	• Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider • Non-Configurable: 2463 used to set RPC sessions to the storage controller from SMI-S provider.
Communication	• See the STM Ports section below. • Can be HTTP/HTTPS between proxy agent and the LSI Engenio SMI-S provider.
NetApp	
Versions/Models	All
Features	Asset Storage Performance
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• IP Address of NetApp head/cluster node • Define user account on NetApp. Minimum access -

	a role with access to execute specific API calls. List available upon request. Usually provided just the root login • Add Proxy agent to list of trusted hosts on the NetApp storage system • ONTAP 7.3.x: Turn off API XML validation on each filer (FAQ-132)
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	• 80 (HTTP)/443 (HTTPS) on NetApp head/cluster node • Any available for CIFS/NFS
Communication	• See the STM Ports section below. • Can be HTTP/HTTPS between proxy agent and the NetApp head/cluster node
SUN/StorageTek	
Versions/Models	All
Features	Asset Storage Performance Disk Performance
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows or UNIX
Prerequisites	• IP Address of Storage Processors • Latest LSI Engenio SMI-S Provider installed on a 32 bit Windows/UNIX server that has IP connectivity to the storage processors
Credentials	Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	• Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider • Non-Configurable: 2463 used to set RPC sessions to the storage controller from SMI-S provider.
Communication	• See the STM Ports section below. • Can be HTTP/HTTPS between proxy agent and the LSI Engenio SMI-S provider.

The following chapter details how to add arrays to monitor. Select your device from the list below.

- IBM 3xxx,4xxx,5xxx Arrays
- IBM SVC
- EMC CLARiiON
- Hitachi
- HP 3PAR
- NetAPP
- NetAPP Flier
- Pillar

Monitoring IBM 3xxx,4xxx,5xxx Arrays

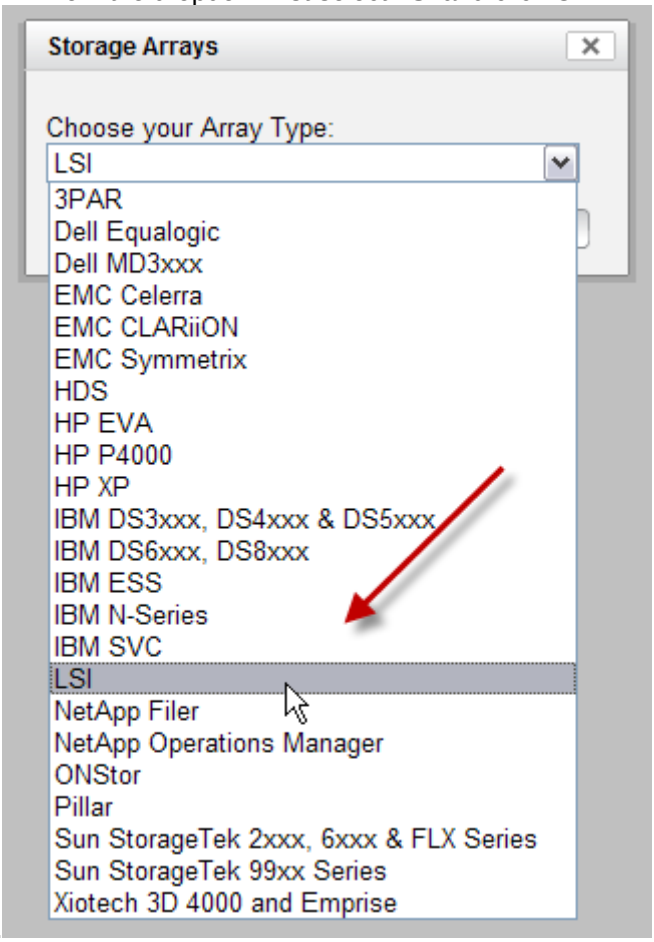
The following section details how to add storage arrays from various vendors.

Note: To add an IBM V7000, you need to select IBM SVC from the dropdown list.

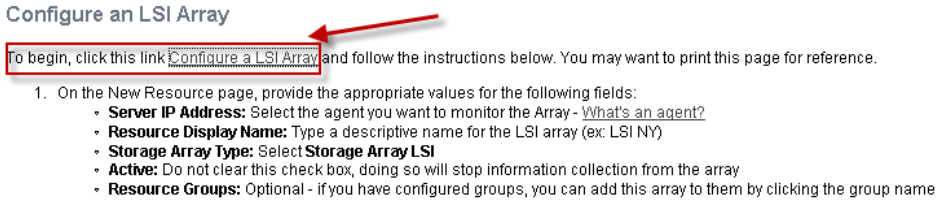
To add a LSI storage array:

1. From the Home page on the STM Web Console Navigate to > **Storage Arrays > click Add**

2. From the dropdown list select LSI and click **OK**.



3. Click the **Configure a LSI Array** link.


Configure an LSI Array
To begin, click this link Configure a LSI Array and follow the instructions below. You may want to print this page for reference.
1. On the New Resource page, provide the appropriate values for the following fields:
Server IP Address: Select the agent you want to monitor the Array - What's an agent?
Resource Display Name: Type a descriptive name for the LSI array (ex: LSI NY)
Storage Array Type: Select Storage Array LSI
Active: Do not clear this check box, doing so will stop information collection from the array
Resource Groups: Optional - if you have configured groups, you can add this array to them by clicking the group name

4. Enter the following selections:

a. **Server IP Address:** Select the agent you want to monitor the Array -

b. **Device Display Name:** Type a descriptive name for the LSI array (ex: LSI NY)

c. **Storage Array Type:** Select **Storage Array LSI**

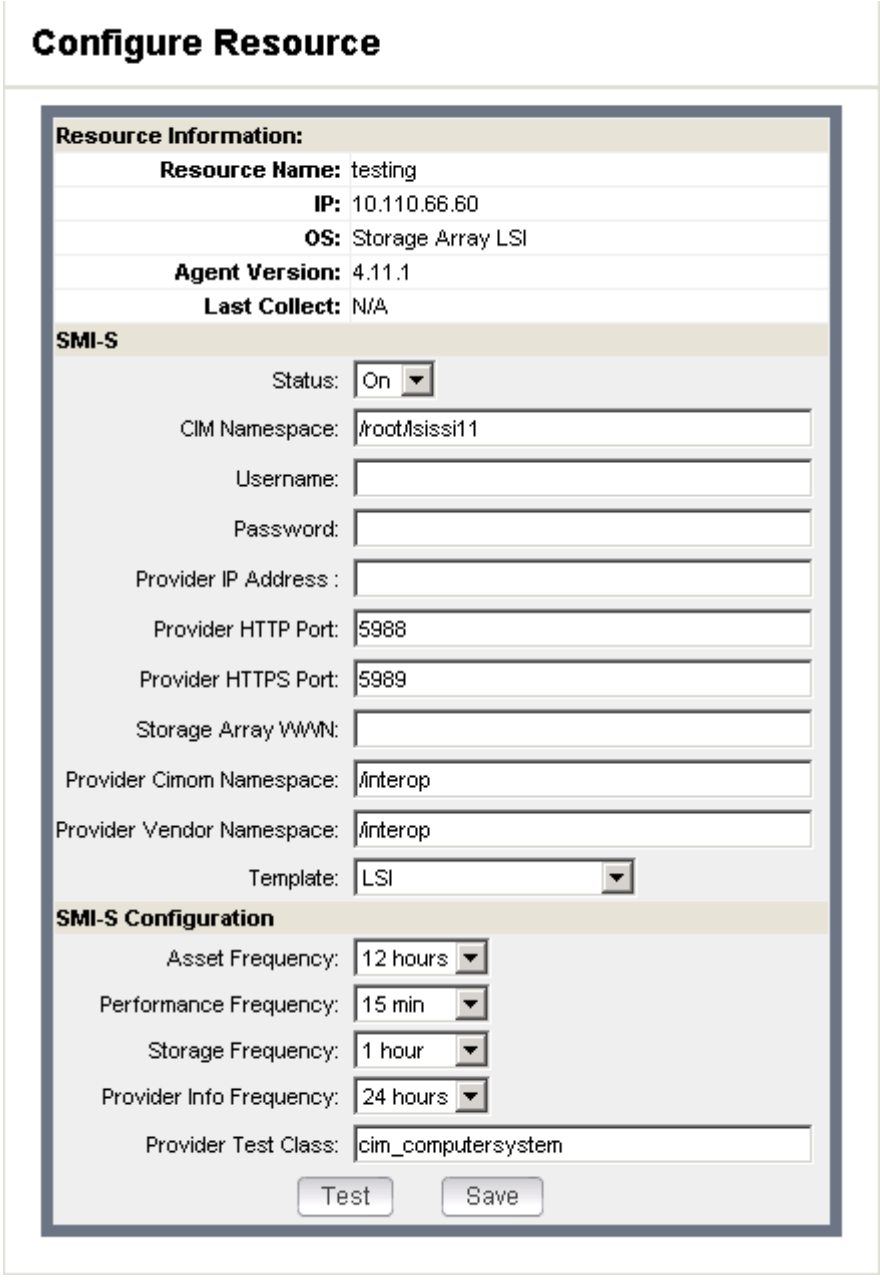
d. **Active:** Do not clear this check box, doing so will stop information collection from the array

e. **Device Groups:** Optional - if you have configured groups, you can add this array to them by clicking the group name

5. Click **Next>** to continue to the next configuration screen.

Provide the appropriate information about the array you want to monitor. If you are unsure about a value, do not change the value from the default.

- **Status:** Select On
- **User Name:** Type the user name used to access the provider
- **Password:** Type the password used to access the provider
- **Provider IP Address:** Type the IP address of the provider
- **Storage Array WWN**: Type the array identifier (the WWN of the LSI array)



6. Click **Save** to save the configuration and push it out to the agent to begin monitoring the array.

Note: Click **Test** to test the connectivity between the agent and provider, and if successful, display the identifiers from the arrays configured in the provider. Note you must have entered the username, password and provider IP address before pressing this .

Monitoring EMC CLARiiON Arrays

The following items are required before you begin:

The EMC SMI-S Provider is installed, running and configured to monitor the Clariion(s) in the environment.

Verify that you have:

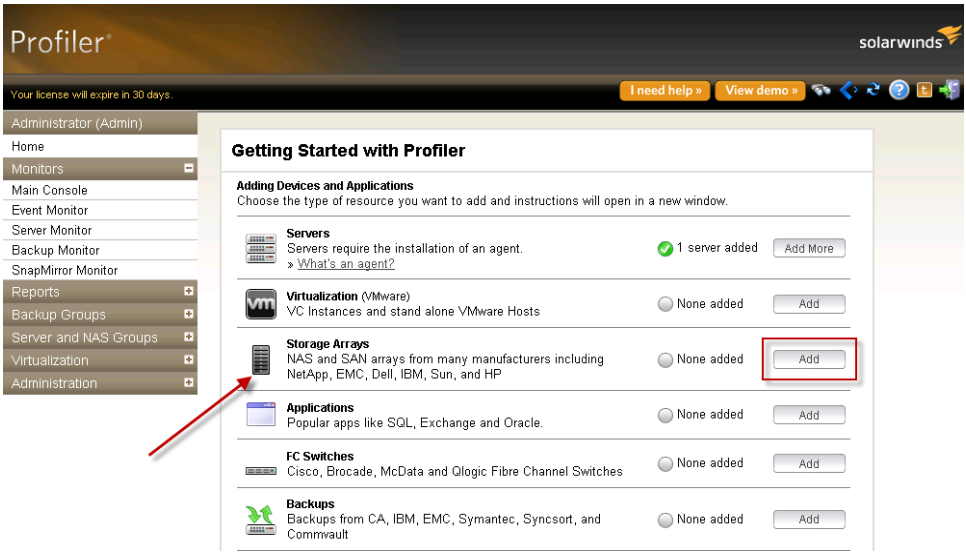
- **a.** EMC SMI-S provider login credentials
- **b.** The IP address of server where the provider is installed
- **c.** The array identifier, which is the serial number of the Clariion array (Ex: Clariion+APM########)
- **d.** WWN (World Wide Name: a unique identifier for a target in a storage network fabric.)

Note: EMC VNX is supported in STM 5.0 and can monitor both the Clariion and Celerra side.

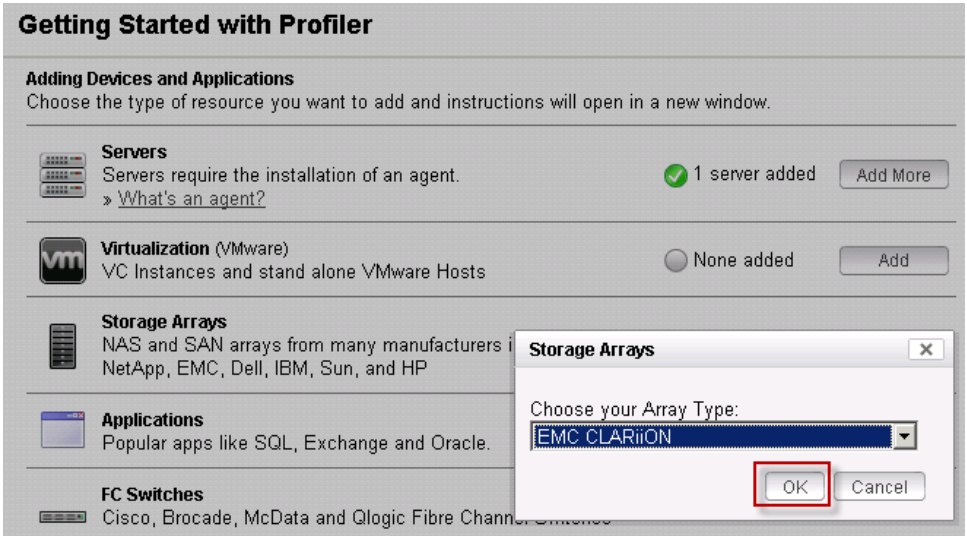
STM provides no mapping between block storage and file systems. To add an **EMC VNX** array, select **Clariion** from the dropdown list.

To begin to configuring an EMC CLARiiON

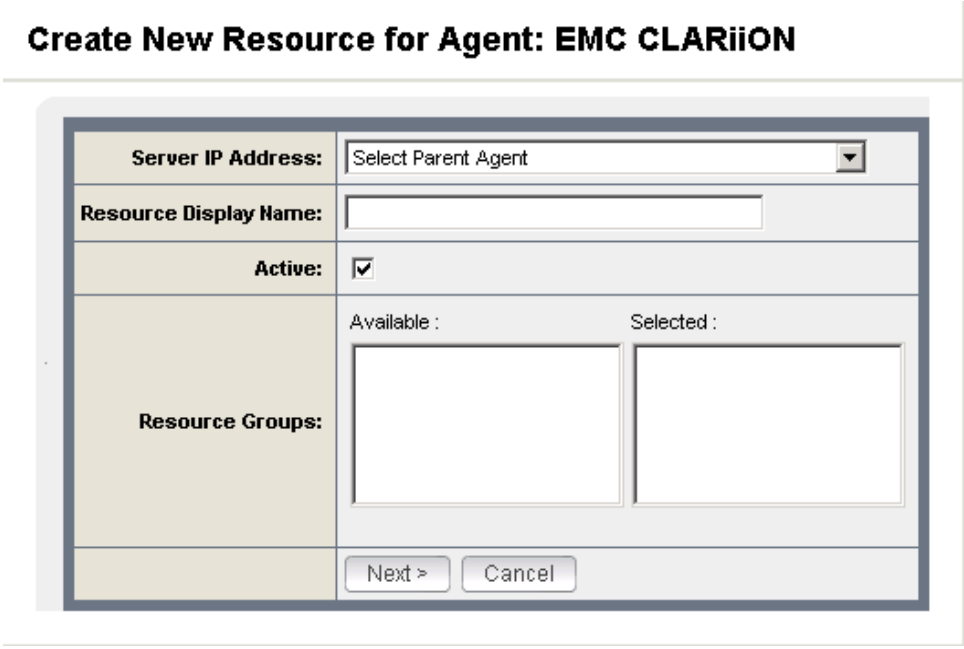
1. From the **Home** page on the Web Console > under **Storage Arrays**> click **Add**



2. Select the Array type from the dropdown, click **OK**

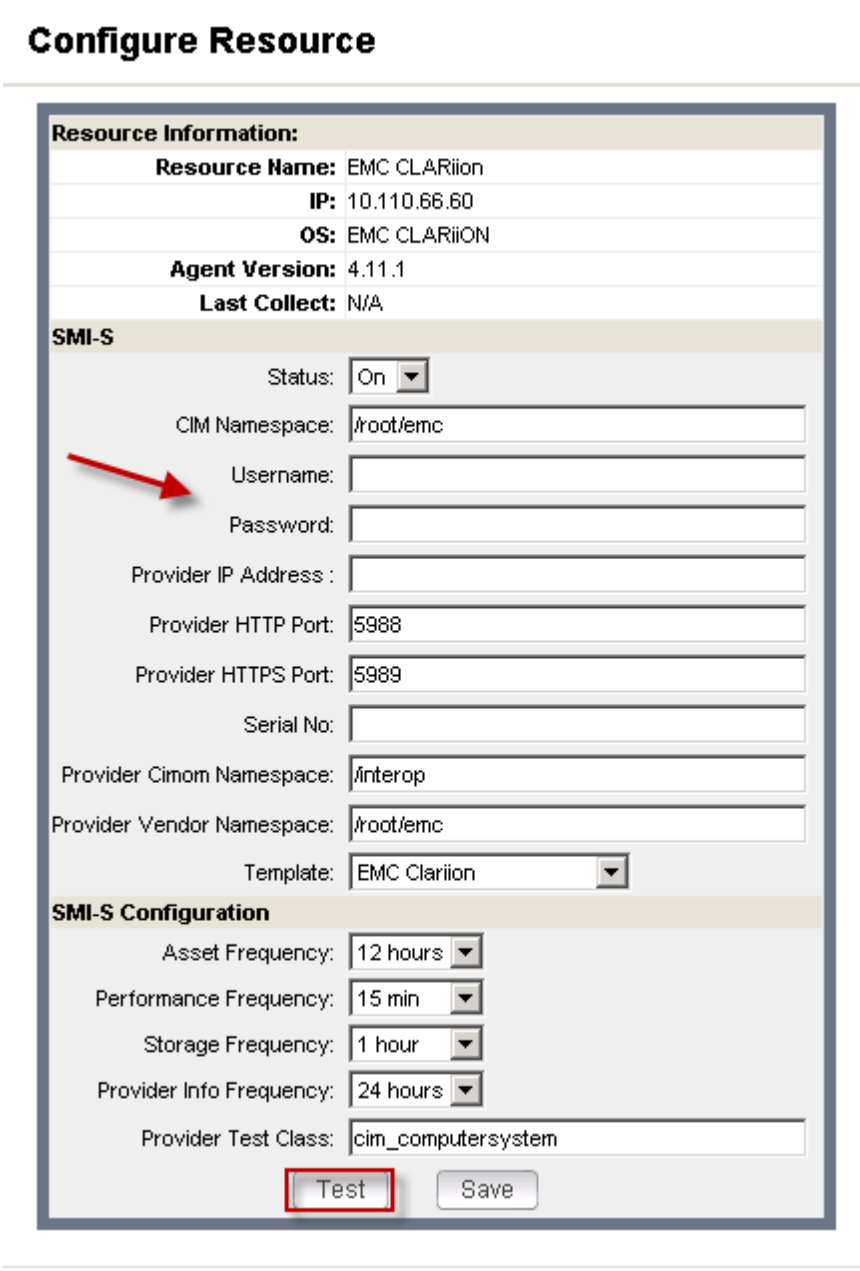

Getting Started with Profiler
Adding Devices and Applications
Choose the type of resource you want to add and instructions will open in a new window.
Servers
Servers require the installation of an agent.
» What's an agent?
1 server added
Add More
Virtualization (VMware)
VC Instances and stand alone VMware Hosts
None added
Add
Storage Arrays
NAS and SAN arrays from many manufacturers i
NetApp, EMC, Dell, IBM, Sun, and HP
Applications
Popular apps like SQL, Exchange and Oracle.
FC Switches
Cisco, Brocade, McData and Qlogic Fibre Chann
Storage Arrays
Choose your Array Type:
EMC CLARiiON
OK
Cancel

3. On the **New Device** page, provide the appropriate values for the following fields:



- **Server IP Address:** Select the agent you want to monitor the Array -
- **Device Display Name:** Type a descriptive name for the Clariion array (ex: Clariion NY1)
- **Active:** Do not clear this check box; doing so will stop data collection from the array
- **Device Groups:** Optional - if you have configured groups, you can add this array to them by clicking the group name

4. Click **Next>** to continue to the next configuration screen.



Provide the appropriate information about the array you want to monitor. If you are unsure about a value, do not change the value from the default.

- **Status**: Select On

- **User Name**: Type the user name used to access the provider
- **Password**: Type the password used to access the provider
- **Provider IP Address**: Type the IP address of the server where the provider is installed
- **Serial Number**: Type the array identifier (the serial number of ClariiON - Ex: ClariiON+APM########)

5. Click **Save** to save the configuration and push it out to the agent to begin monitoring the array.

Notes: Click **Test** to test the connectivity between the agent and provider, and if successful, display the identifiers from the arrays configured in the provider.

You must have entered the username, password and provider IP address before pressing this .

You can also configure arrays on the Devices page (Settings > Devices).

Monitoring NetApp Operations Manager

The following items are required before you begin:

- DFM Server IP address
- DFM Server login with GlobalFullControl privileges
- Ensure that the NetApp Filers are accessible to DFM Server via http/https

Note: DFM Operations Manager which discovers all NetApp Filers.

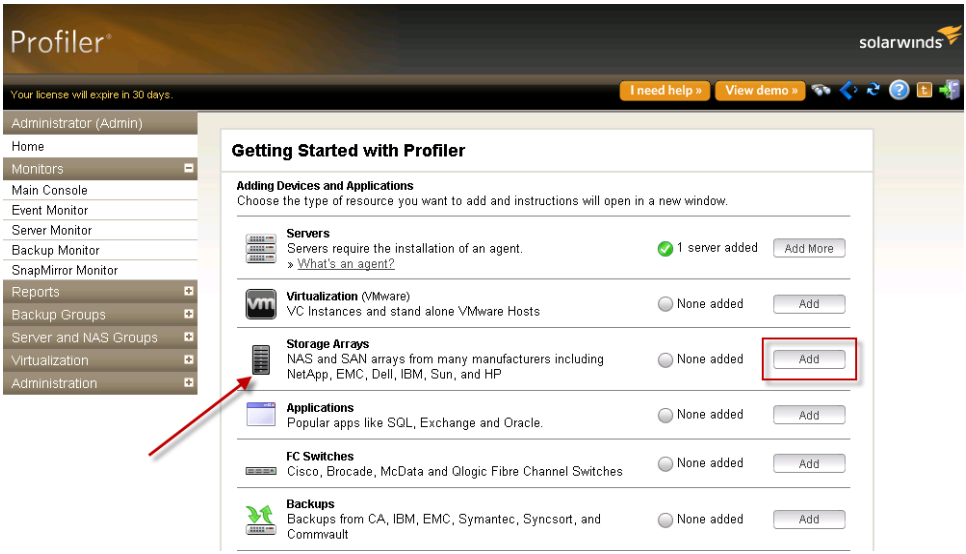
IMPORTANT: Configuring STM to monitor your NetApp infrastructure is a two step process.

1. First, STM must connect to the NetApp Operations Manager to discover all the Filers it is managing.

2. Second, you must select which Filers to monitor and assign them to an agent for data collection. Discovery can take a few minutes in large environments.

To begin to configuring an NetApp

1. From the Home page on the Web Console > under Storage Arrays> click Add



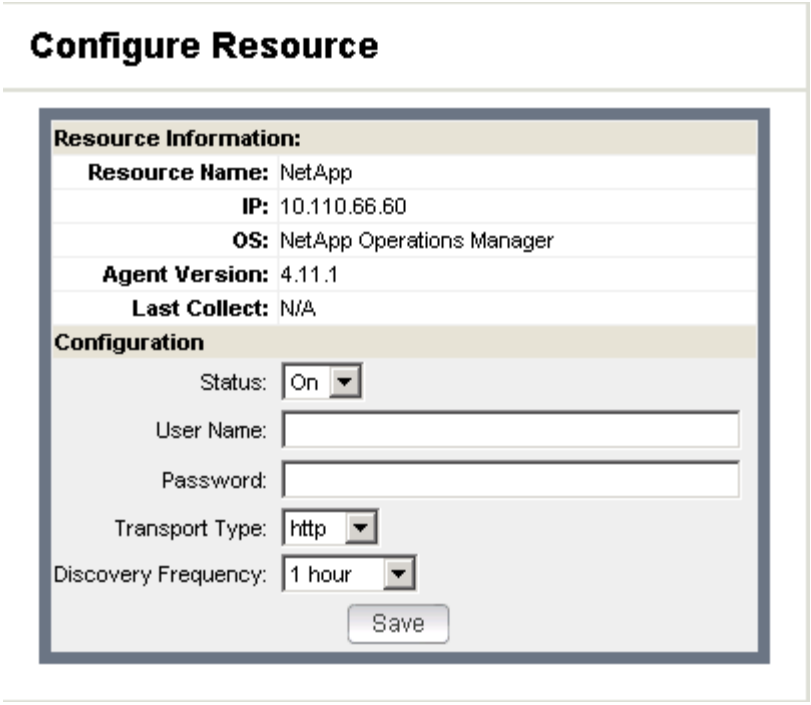
2. Select the Array type from the dropdown, click **OK,** then click **Configure a NetApp Operations Manager.**

Step 1: Configuring a NetApp Operations Manager
To begin, click the link Configure a NetApp Operations Manager and follow the inst
1. On the New Resource page, provide the appropriate values for the following
Select Agent: Select the agent you want to monitor the NetApp Oper
Resource Display Name: Type a descriptive name for the NetApp O
DFM Server IP Address : Type the IP address of the DFM server

3. On the New Device page, provide the appropriate values for the following fields:
   - **Select Agent:** Select the agent you want to monitor the Array -
   - **Device Display Name:** Type a descriptive name for the ClariiON array (ex: ClariiON NY1)
   - **DFM Server IP Address:**
   - **Device Groups:** Optional - if you have configured groups, you can add this array to them by clicking the group name
4. Click **Next>** to continue to the next configuration screen.

Provide the appropriate information about the array you want to monitor. If you are unsure about a value, do not change the value from the default.

- **Status**: Select On
- **User Name**: Type the user name used to access the provider
- **Password**: Type the password used to access the provider
- **Provider IP Address**: Type the IP address of the server where the provider is installed
- **Serial Number**: Type the array identifier (the serial number of ClariiON - Ex: ClariiON+APM########)



5. Click Save to save the configuration and push it out to the agent to begin monitoring the array.

Notes: Click **Test** to test the connectivity between the agent and provider, and if successful, display the identifiers from the arrays configured in the provider. Note you must have entered the username, password and provider IP address before pressing this .

You can also configure arrays on the Devices page (Settings > Devices).

Monitoring NetAPP Filer

The process of adding NetApp is made easier in STM, using the DFM Operations Manager which discovers all NetApps. This functionality is very much similar to Adding ESX Hosts.

Once NetApp has been discovered by the Operations Manager, the NetApp filers can be assigned to the desired Proxy Agent for data collection. To Assign NetApp filers to the proxy Agent, go to Settings -> NetApp Operations Manager -> Assign NetApp Filers page.

Assigning NetApp Filers:

1. Select the **DFM Server**
2. Select the NetApp Filers from "**Available**" box. You can select more than one by holding the control key while selecting.
3. Select the proxy agent.
4. Click the down arrow to move the NetApp Filers down to the **Selected** box.
5. Click **Save**. When you save the change, a push will be scheduled immediately to update the agent(s) with the changes.

Monitoring Hitachi Data Systems

Hitachi Data Systems Sub-Agents can be defined and assigned to an OS Agent when the agent is able to communicate to a SMI-S Provider (provided by the SAN vendor). That SMI-S Provider must be able to communicate with the Storage Array. A single agent device can monitor multiple Hitachi Data Systems devices. The Hitachi Data Systems devices that the Hitachi Data Systems Agent can monitor are:

Hitachi Data Systems (Windows and Solaris Agents only)

3Par, Pillar, IBM SVC

Some Providers are embedded in the device (3par, Pillar, IBM SVC). For these devices, there is no separate Provider to install

3Par

The 3PAR Provider is embedded into the Storage Array.

- The 3PAR InformOS should be 2.3.1 or later
- Need the userid and password
- Need the array IP Address

Pillar

The Pillar SMI Provider is embedded in the array, so there no separate installation required. Upgrades for the Provider are bundled with system software upgrades.

In older Pillar Axiom systems with the 512 MB Pilot hardware, the Provider is disabled by default. Pillar **does not recommend** enabling the SMI Provider if the customer has the older 512 MB Pilots, but recommends upgrading to the 2 GB versions if you want to use the SMI Provider.

The SMI Provider is enabled by default on systems with 2 GB Pilots.

IBM SVC

The IBM SAN Volume Controller (SVC) SMI Provider is embedded in the Management Console software.

All SVC's are sold with a Management Console in the rack on which the SVC GUI is installed to run the proxy server along with a number of other management tools. The Management Console itself is a CIM Client.

SVC CIM Agent Support Matrix: http://www-1.ibm.com/support/docview.wss?rs=591&uid=ssg1S1002888#_SVC_and_SVC

a. The user can stop it and run it once again, and the profile the user has just created will be selected, then check the default profile check box that will make it a default profile.

b. If the MAPI Profile is created successfully, then the executable will continue to run and output mailbox information to the command line.

c. Wait for a few seconds to make sure it is collecting data, then the press Ctrl-C to stop the exe.

d. Next, start the agent.

Monitoring Fibre Channel Devices

The following section details how to add Fibre Channel Switches to STM.

Configuring Fibre Channel Switches

.

To configure a FibreChannel switch from vendors like Brocade, Cisco, McDATA,and Qlogic, ensure you meet the appropriate requirements and complete the following steps.

Requirements

The following items are required before you begin:

- Switch IP Address. This IP must be accessible via telnet from the selected Windows Agent to collect Zoning information from Brocade Switches
- An SNMP v1 read-only community string

Fibre Channel Switches Requirements

- Cisco MDS Switches
- Brocade, McData, and QLogic Switches

Cisco MDS	
Versions/Models	Any
Features	Asset Storage Performance Topology (Tabular)
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows/UNIX Topology requires Windows agent on a SAN attached host to any switch in the fabric.
Prerequisites	• Create SNMP version 1 community string from command line • If there is an access list for SNMP on the switch, include proxy agent(s)'s IP address to the list
Credentials	SNMP community string for each FC Switch
Read/Write Actions	Read Only
Ports Used	161 UDP on the switch
Communication	See the STM Ports section below
Brocade, McData, and QLogic Switches	
Versions/Models	Any
Features	Asset Storage Performance Topology (Tabular) Zoning
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows/UNIX Topology requires Windows agent on a SAN attached host to any switch in the fabric.
Prerequisites	• Enable FA-MIB on switches (on Brocade, command to run is snmpmibcapset) • If there is an access list for SNMP on the switch,

	include proxy agent(s)'s IP address to the list
Credentials	• SNMP community string for each FC Switch • Zoning (v4.8+): Login and Password (telnet) for each FC Switch
Read/Write Actions	Read Only
Ports Used	161 UDP on the switch
Communication	See the STM Ports section below

Community String

- SNMP V1 needs to be enabled to collect data from a CISCO switch.
- If the community string is defined from any CISCO Device/Fabric Manager, then its implicitly for SNMP V3.
- The community string MUST be defined from the command line.

Storage Manager can monitor any switch (or device) that supports the Fibre Alliance MIB. Some switches (for example, McDATA) use an alternate MIB, called the Fibre Channel Management MIB, that provides the same information. For those switches using this MIB, you must check the McDATA box when creating the device. If you are unsure, create the device without checking the box first. If you do not see data after 15-30 minutes, try checking the box and see if data begins to be collected.

Note: To set up Brocade switches, one has to execute the following commands to change the SNMP configuration:

- To enable FA MIB: *`snmpConfig --set snmpv1`*
- For access control: *`snmpConfig --set accessControl`*
- To check: *`snmpconfig: snmpConfig --show`*

To configure a McData Fibre Channel Switch Device:

1. On the new device page enter the appropriate values.

- **Select Agent:** Select the agent you want to monitor the Fibre Channel
- **Switch IP Address:** Type the IP address of the switch
- **Device Display Name:** Type a descriptive name for the Fibre Channel (ex: FC NY1)
- **Active:** Do not clear this check box, doing so will stop information collection from the Fibre Channel

- **McDATA Switch:** Check this if the device uses the FIBRE-CHANNEL-MGMT MIB rather than the standard Fibre Alliance MIB (for example, McDATA switches use this MIB).

Note: McData i10K series switches do not require the McData checkbox to be enabled**.** For more information see this KB article.

- **Device Groups:** Optional - if you have configured groups, you can add this Fibre Channel Switch to them by clicking the group name
- **Zoning:** Check this box and provide credentials, which will generate the Zoning reports.

Note: Zoning option is supported via a Windows Agent only.

2. Click **Next>** to continue to the next configuration screen.
3. Provide the appropriate information about the Fibre Channel switch you want to monitor. If you are unsure about a value, do not change the value from the default.
   a. Status : Select On
   b. SNMP Community String : An SNMP v1 read-only community string
4. Click **Save** to save the configuration and push it out to the agent to begin monitoring the Fibre Channel.

Note: Click **Test** to test SNMP communication between the agent and the Fibre Channel Switch device. You must select an agent, enter a SNMP community string and device IP address, before you press this button.

Chapter 6

Backup Profiler

The Backup Console summarizes a backup cycle (24-hour period that begins at the start of the backup window) for a single backup server or a group of clients.

To configure Backup Profiler to monitor devices, select your device from the list below:

- CA Arcserve
- CommVault Galaxy
- IBM TSM
- EMC Legato
- Symantec Backup Exec
- Symantec NetBackup

Note: Backup Profiler requires purchase and is licensed into two categories.

- **Category 1**: Backup Exec, Arcserve, Commvault
- **Category 2:** Legato, TSM, NetBackup

Configuring the CA Arcserve

To configure, ensure you meet the appropriate requirements and complete the following tasks.

Requirements:

The following items are required before you begin:

- Supported versions: CA ARCServe 2000, 9, 10.x, 11.x (Windows and NetWare),12, 12.5 (Windows) & 11.5 on Linux
- A Storage Manager OS agent must be installed on the ARCServe server.
- For ARCServe on Linux OS and for ARCServe on Windows OS running version 12 and later, the agent should be running under an account service that has appropriate equivalence with the caroot user account of ARCServe.

- Equivalence can be set using the following command from the windows command line: (If you are logged in as a user who has no equivalence to any CA ARCServe Backup user, then you must be granted an equivalence before you can use ca_auth)
- ca_auth -equiv add ntuser hostName ARCServeUser [caroot_username] [caroot_password]

For ARCServe on Linux, create an equivalence of user on hostname to causer:

ca_auth -equiv add UnixUser hostname BrightStorUser [Brightstor_username password]

To execute the agent under this account:

1. Open up the Microsoft Windows Services console.
2. Locate the agent service, right-click and select **Properties**.
3. In the Properties window, select the **Log On** tab.
4. Select the account radio button, and fill in the user account information, under which you would like the agent to run.
5. Click **Apply** and **OK**. You may see a box similar to the following, stating that the user account was granted permission to run as a service. If so, please click OK.

To begin configuring your device: follow the instructions below.

1. On the New Device page, provide the appropriate values for the following fields:

a. **Server IP Address:** Select the agent you want to monitor

b. **Device Display Name:** Type a descriptive name for the ARCServe device (ex: ARCServe NY)

c. **Timezone:** Select the timezone of the Backup Server

d. **Backup Start Window:** Select the Backup start time. This should be the approximate time backup jobs start for the day. If backups run all day, define a 24 hour window.

e. **Backup Window End:** Select the Backup end time

f. **Active:** Do not clear this check box, doing so will stop information collection

g. **Device Groups: Optional** - if you have configured groups, you can add this backup server to them by clicking the group name

h. **Licensing:** Check this box if you want to assign a license to this device

i. **Location:** Type the location

j. **Comment:** Type the comment

2. Click **Next** to continue to the next configuration screen.

Note: If the Storage Manager Agent is not running, it will display a message saying **Could not connect to the Agent**. In this case, please start that Agent and repeat the above procedure.

1. Provide the appropriate information about the backup agent you want to monitor. If you are unsure about a value, do not change the value from the default.

   a. Monitor Backup Server : Select On

   b. Level of the Log : Select Info

   c. Date Format : Enter the Date format as seen in the ARCServe job log. Default is set to MM/dd/yy.

   d. If ARCServe is on Windows and the version is 11.5 or below, enter the date format as seen in the "Start Time "line in the job log.It can be set to MM/dd/yy or dd/MM/yy or yy/MM/dd. Example: the date format would be MM/dd/yy for Start Time..... 3/24/08 6:13 PM

   e. If ARCServe is on Windows and the version is 12 or above (or) ARCServe is on Linux, enter the date format as seen in the START TIME column of the following command's output: ca_dbmgr -show jobs -last 3 days

Example: the date format would be MM/dd/yy for the following outputs:

No	Job Id	Job Type	Job Status	Job Owner	Start Time	End Time	Set Name
1	13	Backup	Finished	Caroot	**1/30/2009 11:32:14 AM**	**1/30/2009 11:34:34 AM**	

No	Job Id	Job No	Job Type	Job Status	Job Owner	Start Time	End Time	Set Name	Duration (hh:mm:ss)	Comments
1	8	8	Backup	Finished	Caroot	**03/24/09 11:19**	03/24/09 11:20		00:00:38	JobFullBackup

If ARCServe is on Netware enter the date format as seen in the start of a line in the job log. It can be set to MM/dd/yy or dd/MM/yy.

For example: The date format would be MM/dd/yy for **"Aug-01 23:30:10"** and dd/MM/yy for **"01-Aug 23:30:10"**

1. Click Save to save the configuration and push it out to the agent to begin monitoring the device.

Configuring CommVault Galaxy

To configure, ensure you meet the appropriate requirements and complete the following tasks.

Requirements:

The following items are required before you begin:

- Supported versions: CommVault Galaxy 7.x and 8.x
- A Storage Manager OS agent is required on the CommVault server if error and exception information is desired.

Configuring CommVault Galaxy

To begin, follow the instructions below. .

1. On the New Device page, provide the appropriate values for the following fields:
    - **Server IP Address:** Select the agent you want to monitor
    - **Device Display Name:** Type a descriptive name for the CommVault Galaxy device (ex: Commvault NY)
    - **Timezone:** Select the timezone of the Backup Server
    - **Backup Start Window:** Select the Backup start time. This should be the approximate time backup jobs start for the day. If backups run all day, define a 24 hour window.
    - **Backup Window End:** Select the Backup end time
    - **Active:** Do not clear this check box, doing so will stop information collection
    - **Device Groups:** Optional - if you have configured groups, you can add this backup server to them by clicking the group name
    - **Licensing:** Check this box if you want to assign a license to this device
2. Click **Next>** to continue to the next configuration screen.
3. Provide the appropriate information about the backup agent you want to monitor. If you are unsure about a value, do not change the value from the default.
    - Monitor Backup Server : Select On
    - Level of the Log : Select Info
    - Install Dir : Type the path to where CommVault Galaxy is installed [default path is: C:\Program Files\CommVault\Galaxy]
    - Job Manager File Path : Type the Commvault Job Manager file path [default path is: C:\Program Files\CommVault\Galaxy\Log Files\JobManager.log]
    - Exception Frequency : Select the frequency for gathering activity info [default is: 10 min]
    - Configuration Frequency : Select the frequency for gathering configuration info [default is: 3 hours]
    - MS-SQL Server Name : Type the Name of the MS-SQL Server containing the CommVault database.This value is required only if you want to monitor missed jobs
    - CommVault Database Name : Type the name of the CommVault Database. Type: CommServ

- CommVault Database Port: Database Port. This can be found by checking the Dynamic Port under the TCP IP properties in SQL Network Configuration Manager where the CommVault SQL database resides.
- CommVault Database Username: Type the username to connect to this CommVault Database. This can be a local account or domain account
- CommVault Database Password: Type the password for this UserName.
- Domain: Type the domain associated with this UserName. Leave the field blank if using a local server account.
- CommVault Database Polling Frequency: Frequency to poll CommVault Database for missed jobs. [default is: 10 min]
- Error Codes: Select the error codes for which you would like the agent to send a monitoring trap on.

4. Click **Save** to save the configuration and push it out to the agent to begin monitoring the device.

Configuring the IBM TSM

To configure, ensure you meet the appropriate requirements and complete the following tasks.

Requirements

The following items are required before you begin:

- Supported versions: IBM TSM Backup Servers 5.0, 5.1, 5.2, 5.4, 6.1 (AIX, Solaris, HP-UX , Linux and Windows)
- TSM Instance name - The server name as specified in dsm.opt file on windows and dsm.sys file on Unix
- TSM login credentials

Configuring IBM TSM

To begin, click this link Configure an IBM TSM Backup Agent and follow the instructions below. .

1. On the New Device page, provide the appropriate values for the following fields:

- **Server IP Address:** Select the agent you want to monitor
- **Device Display Name:** Type a descriptive name for the IBM TSM device (ex: IBM TSM NY)
- **Timezone:** Select the timezone of the Backup Server

- **Backup Start Window:** Select the Backup start time. This should be the approximate time backup jobs start for the day. If backups run all day, define a 24 hour window.
- **Backup Window End:** Select the Backup end time
- **Active:** Do not clear this check box, doing so will stop information collection
- **Device Groups:** Optional - if you have configured groups, you can add this backup server to them by clicking the group name
- **Licensing:** Check this box if you want to assign a license to this device

2. Click **Save**
3. Provide the appropriate information about the backup agent you want to monitor. If you are unsure about a value, do not change the value from the default.
    - Monitor Backup Server : Select On
    - Level of the Log : Select Info
    - TSM Instance Status : If there are multiple TSM instances defined on the same server and want to disable one of them , change it to Off.
    - TSM Instance Name : Type the instance name. It is the server name as specified in dsm.opt file on windows and dsm.sys file on Unix.

For Example: TSM instance name will be MEY_SERVER1 as specified in Servername value

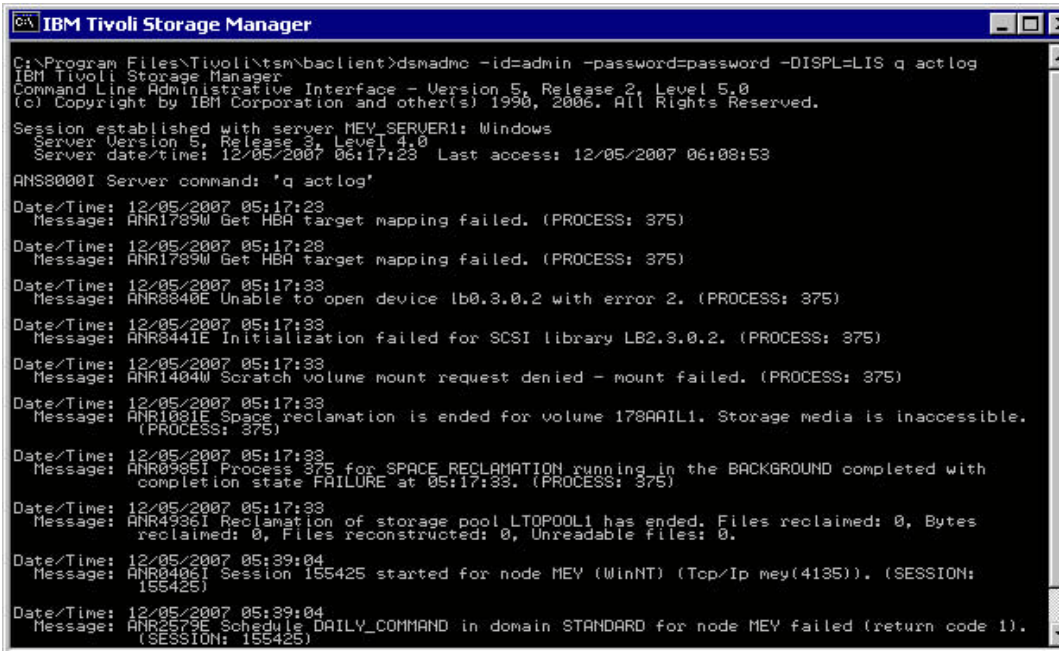
```
TCPSERVERADDRESS localhost
servername      MEY_SERVER1
NODENAME        mey2
```

Instance name is Case Sensitive

- **Path of dsmadmc Executable :** Type the path to the directory where the "dsmadmc" executable file is present
  (ex., the default path in Windows is "C:\Program Files\tivoli\tsm\baclient" and default path in Unix is "/usr/tivoli/tsm/client/ba/bin").
- **Username :** Type the user name to log into TSM.
- **Password :** Type the password to log into TSM.
- **Date Format :** Type the date format as seen in the actlog query output. (Default MM/dd/yyyy)

For Example: Run the following command on the TSM server and Note down the dateformat from the output and type it during TSM configuration

dsmadmc id = < username > -password = < password > q actlog
the output looks like
Date format will be MM/dd/yyyy and Time format will be HH:mm:ss


IBM Tivoli Storage Manager
C:\Program Files\Tivoli\tsm\baclient>dsmadmc -id=admin -password=password -DISPL=LIS q actlog
IBM Tivoli Storage Manager
Command Line Administrative Interface - Version 5, Release 2, Level 5.0
(c) Copyright by IBM Corporation and other(s) 1990, 2006. All Rights Reserved.
Session established with server MEY_SERVER1: Windows
Server Version 5, Release 3, Level 4.0
Server date/time: 12/05/2007 06:17:23 Last access: 12/05/2007 06:08:53
ANS8000I Server command: 'q actlog'
Date/Time: 12/05/2007 05:17:23
Message: ANR1789W Get HBA target mapping failed. (PROCESS: 375)
Date/Time: 12/05/2007 05:17:28
Message: ANR1789W Get HBA target mapping failed. (PROCESS: 375)
Date/Time: 12/05/2007 05:17:33
Message: ANR8840E Unable to open device lb0.3.0.2 with error 2. (PROCESS: 375)
Date/Time: 12/05/2007 05:17:33
Message: ANR8441E Initialization failed for SCSI library LB2.3.0.2. (PROCESS: 375)
Date/Time: 12/05/2007 05:17:33
Message: ANR1404W Scratch volume mount request denied - mount failed. (PROCESS: 375)
Date/Time: 12/05/2007 05:17:33
Message: ANR1081E Space reclamation is ended for volume 178AAIL1. Storage media is inaccessible.
(PROCESS: 375)
Date/Time: 12/05/2007 05:17:33
Message: ANR0985I Process 375 for SPACE RECLAMATION running in the BACKGROUND completed with
completion state FAILURE at 05:17:33. (PROCESS: 375)
Date/Time: 12/05/2007 05:17:33
Message: ANR4936I Reclamation of storage pool LTOPOOL1 has ended. Files reclaimed: 0, Bytes
reclaimed: 0, Files reconstructed: 0, Unreadable files: 0.
Date/Time: 12/05/2007 05:39:04
Message: ANR0406I Session 155425 started for node MEY (WinNT) (Tcp/Ip mey(4135)). (SESSION:
155425)
Date/Time: 12/05/2007 05:39:04
Message: ANR2579E Schedule DAILY_COMMAND in domain STANDARD for node MEY failed (return code 1).
(SESSION: 155425)

- **Time Format:** Type the time format as seen in the actlog query output as shown in the above example. (Default HH:mm:ss)
- **Activity Frequency:** Select the frequency to monitor the log file (default is 5 mins).
- **Media Frequency:** Select the frequency to monitor the media information.
- **Configuration Frequency:** Select the frequency to monitor configuration data.
- **Occupational Trending Frequency:** Select the Frequency to monitor trending data.
- **TSM DB Threshold:** Select the TSM DB Threshold used for notification.
- **TSM Log Threshold:** Select the TSM Log Threshold used for notification.
- **Scratch Threshold:** Select the TSM Scratch Used Percentage used for notification.
- **DSM Config path:** Type the path to dsm.opt file.

- **DSM Directory path:** Type the Directory path to dsm.opt file.
- **Has Oracle Clients:** If the user wants to combine the RMAN pieces for the Oracle jobs. Then this should be set to true. The configuration settings will have to be saved once for Oracle Client Association Type to be visible.
- **Oracle Client Association Type :** If the user selects the MANUAL option, the configuration settings will have to be saved once for the TSM Association field to become visible with a link to modify the TSM Association details.
- **TSM Association :** If has Oracle clients been set to True, then association should be made. This is mandatory , otherwise activity data will not be seen. Otherwise Has Oracle clients should be set to False. Click the on link to map the DBNodes with FS Nodes. The following fields are required for mapping:
    - **DB Node :** Select the node name as specified in the schedule.(Node name should match as seen in events table)
    - **Associated Node:** Select the Associated node name for the Oracle job.

      Note: If there are different node name for each oracle database, then the association should be made for each database.
    - **Move :** To Move nodes from Available to Selected nodes click on Down arrow button and Move nodes from Selected nodes to Available click on Up arrow button

- **LAN Free Clients:** If there are LAN Free Clients, then move them to selected box.
- **Failed Event Frequency:** Change the frequency to read all the events table for all failures.
- **Show Informational Messages:** You can turn off Server level informational messages by selecting False, which will ignore all the ANR messages with I severity.
- **Send Backup Traps:** Select TRUE or FALSE for Backup Traps to be sent.

- **Enable Server Exception:** You can turn off Server level exceptions messages by selecting False, which will ignore all the ANR messages with I, W, E, D and S severity.

4. Click **Save** to save the configuration and push it out to the agent to begin monitoring the device.

Configuring EMC Legato

1. On the New Device page, provide the appropriate values for the following fields:
   - **Server IP Address:** Select the agent you want to monitor
   - **Device Display Name:** Type a descriptive name for the EMC NetWorker device (ex: EMC NetWorker NY)
   - **Timezone:** Select the timezone of the Backup Server
   - **Backup Start Window:** Select the Backup start time. This should be the approximate time backup jobs start for the day. If backups run all day, define a 24 hour window.
   - **Backup Window End:** Select the Backup end time
   - **Active:** Do not clear this check box, doing so will stop information collection
   - **Device Groups:** Optional - if you have configured groups, you can add this backup server to them by clicking the group name
   - **Licensing:** Check this box if you want to assign a license to this device
2. Click **Next>** to continue to the next configuration screen.
3. Provide the appropriate information about the backup agent you want to monitor. If you are unsure about a value, do not change the value from the default.
   - Monitor Backup Server : Select On
   - Level of the Log : Select Info
   - Install Dir : Type the directory where EMC NetWorker is installed (default on Windows is "C:\Program Files\Legato\nsr", Solaris is "/nsr"). Modify the path if it is not correct.
   - Bin Dir : Type the directory where EMC NetWorker executables are installed (default on Windows is "C:\Program Files\Legato\nsr\bin", Solaris is "/nsr/bin"). Modify the path if it is not correct.
   - Res Dir : Type the directory where EMC NetWorker device files are installed (default on Windows is "C:\Program Files\Legato\nsr\res", Solaris is "/nsr/res"). Modify the path if it is not correct.

- Log Directory : Type the directory where log files are written (default on Windows is "C:\Program Files\Legato\nsr\logs", Solaris is "/nsr/logs"). Modify the path if it is not correct.
- MM Database Dir : Type the directory where the MM database resides (default on Windows is "C:\Program Files\Legato\nsr\mm", Solaris is "/nsr/mm"). Modify the path if it is not correct.
- Index Database Dir : Type the directory where the Index database resides (default on Windows is "C:\Program Files\Legato\nsr\index", Solaris is "/nsr/index"). Modify the path if it is not correct.
- Path to nsradmin : Type the directory where the nsradmin resides (default on windows is "C:\Program files\Legato\nsr\bin", Solaris is "/nsr/bin"). Modify the path if it is not correct.
- Config and Media Frequency : Select the interval to collect configuration and media information (default is 24 hours).
- Log Monitor Frequency : The interval to watch the daemon and messages log files in minutes (default is 5 mins).
- Database Catalog Frequency : Select the interval to watch the database catalog in hours (default is 3 hrs).
- Date Format : Select the date format of your daemon.log (Pre-Networker 7.4) or daemon.raw (Post-NetWorker 7.4). (GMT Example: MM/dd/yy HH:mm:ss) (Meridian AM/PM Example: MM/dd/yy HH:mm:ss a)
- Savegrp/ Message File Path : Type the savegrp.log file name along with the path. If savegroup logs are not enabled type the messages/summary file. This setting is required for version EMC NetWorker 7.3 and above.
- Savegrp/ Message Log Monitor Freq : Select the frequency to monitor the savegrp/messages log file.
- Send Backup notifications : Select true to enable backup traps.
- Has Client Initiated SAP Backups? : Select true if the client has initiated SAP backups.
- Bootstrap Info Monitor Frequency : Select the frequency that will be used to monitor bootstrap info.

4. Click **Save** to save the configuration and push it out to the agent to begin monitoring the device.

Configuring Symantec Backup Exec

To configure, ensure you meet the appropriate requirements and complete the following tasks.

Requirements:

The following items are required before you begin:

- Supported versions: Symantec Backup Exec 8.5, 9, 10, 11, 11.5, 12, 12.5 Servers (Windows and NetWare)
- Configuring Symantec Backup Exec

To begin, click this link Configure a Symantec Backup Exec Sub-Agent and follow the instructions below.

1. On the New Device page, provide the appropriate values for the following fields:
   - **Server IP Address:** Select the agent you want to monitor
   - **Device Display Name:** Type a descriptive name for the Symantec Backup Exec device (ex: BEXEC NY)
   - **Timezone:** Select the timezone of the Backup Server
   - **Backup Start Window:** Select the Backup start time. This should be the approximate time backup jobs start for the day. If backups run all day, define a 24 hour window.
   - **Backup Window End:** Select the Backup end time
   - **Active:** Do not clear this check box, doing so will stop information collection
   - **Device Groups:** Optional - if you have configured groups, you can add this backup server to them by clicking the group name
   - **Licensing:** Check this box if you want to assign a license to this device
2. Click **Next**> to continue to the next configuration screen.
3. Provide the appropriate information about the backup agent you want to monitor. If you are unsure about a value, do not change the value from the default.
   - **Monitor Backup Server**: Select On
   - **Level of the Log**: Select Info
   - **Install Dir:** Type the install directory of Backup Exec (the default on Windows is "C:\Program Files\Symantec\Backup Exec"). Modify the path if it is not correct.
   - **Backup Exec log Directory** : Type the log directory of Backup Exec (the default on windows is "C:\Program Files\Symantec\Backup Exec\NT\Data"

- **Version of Backup Exec**: Select the Backup Exec version from the drop-down menu.
- **Prefix of the Backup Exec Logs:** Type the prefix of the Backup Exec logs.
- **Job DateTime Format** : Type the job date/time format as present in Backup Exec job logs.
  The job time can be got by searching for "Job started" line if Backup Exec is on Windows or "Backup operation started" on Netware.

  For example:

- If Backup Exec is on Windows and the Backup Exec version is 9.x - <start_time> Job started : Monday, January 07, 2008 at 12:00:04 AM </start_time>
- If Backup Exec is on Windows and the Backup Exec version is 8.x - Job started : 30 November 2006 at 20:00:05
- If Backup Exec is on Netware:
  ##NML##Backup operation started : 01/11/08 at 04:00:02a

  Following are some examples showing sample date/time values and the format:

Date/Time	Job Date Time Format
Wednesday, May 09, 2007 at 8:30:11 PM	EEEEE, MMMMM dd, yyyy 'at' hh:mm:ss a
16 March 2006 at 22:00:35	dd MMMMM yyyy 'at' HH:mm:ss
01/14/08 at 04:00:02a	MM/dd/yy 'at' hh:mm:ss a
14/01/08 at 04:00:02p	dd/MM/yy 'at' hh:mm:ss a

o

o Set Date Time Format: Type the set date/time format as present in Backup Exec job logs.
  The set time can be got by searching for "Backup started on" line if Backup Exec is on Windows or "Backup set started" if Backup Exec is on Netware.

  For example:

- If Backup Exec is on Windows and the Backup Exec version is 9.x - <start_time> **Backup started on** 1/7/2008 at 12:00:08 AM. </start_time>

- If Backup Exec is on Windows and the Backup Exec version is 8.x - **Backup started on** 30/11/2006 at 20:01:07.
  3) If Backup Exec is on Netware:
  ##NML##**Backup set started :** 01/11/08 at 06:21:26a

  Following are some examples showing sample date/time values and the format:

Date/Time	Set Date Time Format
5/14/2007 at 8:33:13 PM	MM/dd/yyyy 'at' hh:mm:ss a
16/03/2006 at 22:01:15	dd/MM/yyyy 'at' HH:mm:ss
01/14/08 at 04:00:02a	MM/dd/yy 'at' hh:mm:ss a
14/01/08 at 04:00:02p	dd/MM/yy 'at' hh:mm:ss a

  o **Note: The above two fields cannot be left blank.**

The following values are required only if you want to monitor Backup Exec missed jobs, else leave them as NA

- **MS-SQL Server Name :** Name of the MS-SQL Server containing the Backup Exec database.
- **Backup Exec Database Name :** MS-SQL database name of the Backup Exec database.
- **Backup Exec Database Port :** The port on which this MS-SQL server runs.
- **Backup Exec Database User Name :** MS-SQL user login to connect to this Backup Exec database.
- **Backup Exec Database Password :** Password for this MS-SQL user name.
- **Domain :** Windows Domain associated with this MS-SQL user login if applicable, else leave it as NA.
- **Backup Exec Missed Jobs polling Frequency :** The frequency at which Backup Exec database would be polled for missed jobs.

- **Backup Exec Media polling Frequency :** The frequency at which Backup Exec media would be polled.

4. Click **Save** to save the configuration and push it out to the agent to begin monitoring the device.

Configuring Symantec NetBackup

To configure, ensure you meet the appropriate requirements and complete the following tasks.

Requirements:

The following items are required before you begin:

- Supported versions: Symantec NetBackup 4.5, 5.1.x, 6.1.x, 6.5.2, 6.5.3.x, 6.5.4 Servers (Windows, Solaris, AIX, Linux, HP-UX and Tru64)
- A Storage Manager OS agent must be installed on the NetBackup master server.
- The NetBackup install directory.

Configuring a Symantec NetBackup Server

To begin follow the instructions below.

1. On the New Device page, provide the appropriate values for the following fields:
   - **Server IP Address:** Select the agent you want to monitor
   - **Device Display Name:** Type a descriptive name for the NetBackup device (ex: NetBackup NY)
   - **Timezone:** Select the timezone of the Backup Server
   - **Backup Start Window:** Select the Backup start time. This should be the approximate time backup jobs start for the day. If backups run all day, define a 24 hour window.
   - **Backup Window End:** Select the Backup end time
   - **Active:** Do not clear this check box, doing so will stop information collection
   - **Device Groups:** Optional - if you have configured groups, you can add this backup server to them by clicking the group name
   - **Licensing:** Check this box if you want to assign a license to this device

2. Click **Next>** to continue to the next configuration screen.

Provide the appropriate information about the backup agent you want to monitor. If you are unsure about a value, do not change the value from the default.

- Monitor Backup Server : Select On
- Level of the Log : Select Info
- Install Dir: Type the install directory of NetBackup (the default on Windows is "C:\Program Files\Symantec", on Solaris it is "/usr/openv"). Modify the path if it is not correct. The NetBackup subdirectory name automatically appended to the directory path entered here.
- Activity Frequency: Select the frequency to monitor the log file (default is 5 mins).
- Config and Media Frequency: Selct the frequency to monitor the configuration file (default is 24 hours).
- Get Client Version: Select true to get the version of each NetBackup client.
- Send Backup Notifications: Select false to only get failed backup and downed tape drive traps. Selecting true enables all NetBackup exeception messages to be considered traps.

3. Click **Save** to save the configuration and push it out to the agent to begin monitoring the device.

Chapter 7

Monitoring VMware

This section covers the following topics:

- VMware Configuration
- VMware Requirements
- Virtualization Dashboard

VMware Device Requirements

VMware	
Versions/Models	3.0, 3.0i, 4.0, 4.0i, 4.1, 4.1i
Features	Asset - (VC, Cluster, ESX, and VM levels) Storage - (VC, Cluster, ESX, and VM levels) Performance - (VC, Cluster, ESX, and VM levels) Capacity Planning
Requires Agent?	No
Requires a Proxy Agent?	Yes – Windows or Linux agents Proxy must not be installed on Virtual Center server
Prerequisites	Create user on Virtual Center with a role containing the following privileges • Datastore.browse • Global.Licenses • System.view • System.Anonymous • System.Read
Credentials	• Run as root user on Unix/Linux • Local System account/Domain Account (Windows) • Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	• Virtual Center: HTTPS Port 443 • Profiler Data Collector/Agent Ports
Communication	• Virtual Center uses port 443 by default for HTTPS access. Proxy agent queries VC on this HTTPS port • See the STM Ports section below

The STM Virtualization Dashboard provides quick views into your current virtualized environment including:

- Asset Summary (including Clusters)
- Capacity Analysis
- Storage by type
- Data stores
- VMDK Utilization
- VMs by last boot time
- Storage Utilization by VM
- VMware snapshots
- Overall performance of each device- CPU, Memory, Disk

Capacity Analysis

Capacity Analysis page will display the current usage of CPU, Memory, Storage, Disk and Network per VM as well as per ESX level. It estimates the maximum number of VMs that can be added into the environment based on the target. It also estimates the maximum number of VMs that can be added at emergency.

For example: If the user sets the target utilization as 80% then 20% is allocated to Emergency. In this 20%, the number of VMs that can be added, will be the 'Emergency' VM count.

The 'Host will run out of storage first' is the 'Storage'. If the Current Utilization is 70%, then (80-70=10) For example: 10% is the available storage. In that 10% the number of VMs that can be added, based on the average storage per VM is the 'Available' VM count.

P2V Simulator

P2V (physical to virtual) is the migration of operating systems and their associated applications from physical, dedicated hardware into virtualized environments. The P2V migration can be handled through specialized software tools that automate the process. Or, the P2V migration can be performed manually—for instance, by installing an OS and appropriate applications on an assigned virtual machine.

To access the P2V Simulator:

1. Click **Virtualization > P2V Simulator**
2. Select the group you want to simulate and then click **Go**.
3. Select **Target Group** and a **Physical Server to Virtualize.**

4. Click **Run Report**.

The capacity planning results display a "Before and After" chart similar to the below example.

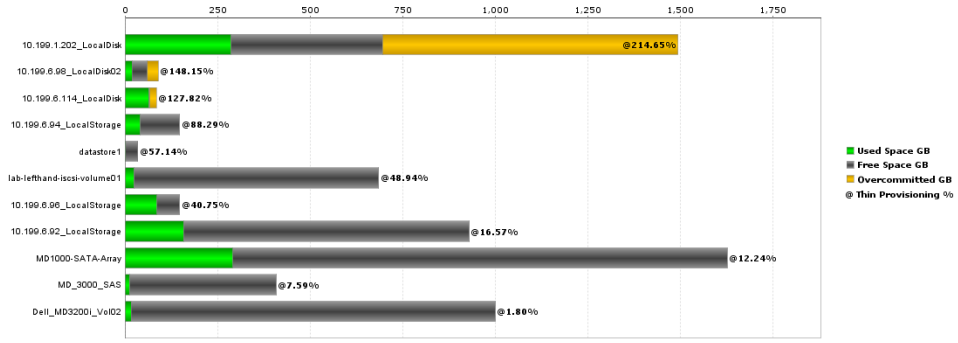
Capacity Planner

Host : Lab(datacenter-2)		
Value :	**Before**	**After**
Total VMs :	376	377
VMs Running :	14	15
CPU Usage % (MHz) :	21.51% (10348MHz)	22.58% (10861MHz)
RAM Usage % (GB) :	44.85% (24.67GB)	52.13% (28.66GB)
Datastore Usage % (GB) :	23.4% (902.07GB)	24.44% (942.05GB)
Dell_MD3200i_Vol02 Usage % (GB) :	1.69% (16.85GB)	5.69% (56.84GB)

Thin Provisioning

Thin provisioning is a system that applies to large scale, centralized computer disk storage systems, SANs, and storage virtualization systems. Thin provisioning allows for administrators to allocate storage space to multiple servers easily and allows distributed storage systems to be deployed as needed provisioning.

The STM Virtualization Dashboard provides a graphical display of your datastore Thin Provisioning. Displays thin provisioning info on virtual disks, so you can see the level of over commitment on your datastores.



The legend for thin provisioning is as follows:

- **Used Space** is the actual amount of space used.
- **Free** is the physical amount of storage still available.
- **Overcommitted** is how much storage is committed above the physical storage available.
- **Thin provisioning percent** is the percentage of over commitment above the physical storage.

Configuring VMware

VMware VC Instances can be monitored from any Storage Manager agent.

A VMware VC Instance can discover the ESX Servers connected to virtual center.

IMPORTANT: Configuring Storage Manager to monitor your virtual infrastructure is a **two step process**.

- First, Storage Manager must connect to the VC instance and discover all the ESX hosts it is managing.
- Second, you must select which ESX hosts to monitor. Discovery can take a few minutes in large environments.

Requirements

The following items are required before you begin:

- A Storage Manager agent located on the same network as the VC instance
- Login credentials to the VC Instance.

Step 1: Configuring a VMware VC Instance

To begin follow the instructions below. .

1. On the New Device page, provide the appropriate values for the following fields:

- **Poller:** Select the poller you want to collector data. A poller is an agent that has been licensed to monitor the VMware infrastructure.
- **Device Display Name:** Type a descriptive name for the VMware VC Instance (ex: VMwareVC NY)
- **VMware VC IP Address:** Type the IP Address of your Virtual Center management console

2. Click **Next>** to continue to the next configuration screen.
3. Provide the appropriate information about the VMware VC Instance you want to monitor. If you are unsure about a value, do not change the value from the default.
    - Status : Select ON
    - UserName : Virtual Centre login [Do not include Windows domain even if this is a domain account]
    - Password : Virtual Centre password
    - Collect Orphaned VMDK : Select Yes unless you do not need reports on orphan VMDK Files
    - Collect Device Pools : Select Yes
4. Click **Save** to save the configuration and push it out to the poller to begin monitoring the VC instance.

Note: You can also configure VMware VC Instance on the Devices page (Settings > All Devices).

Step 2: Assigning VMware ESX Hosts

Once Storage Manager has discovered your ESX Hosts, you can then assign them to a poller for data collection.

If no ESX Hosts are not listed in the Available list after 15 minutes, you may have an authentication problem with vCenter.

Verify your credentials and try again or contact SolarWinds for support. You can always test the authentication yourself from this machine by manually connecting to the vCenter using a web browser: **https://<VC IP Address>/ui**

1. On the Assign ESX Hosts page:

a. Select the Virtual Centre Instance in the top drop down, you should see ESX Hosts appear.

b. Select the ESX Hosts you want to monitor

c. Select the poller you want to use from the drop down list

d. Click the down arrow button to assign the ESX host to the poller and move them to the Selected list below

2. Click Save. This will push the configuration out the selected poller(s) and begin data collection.

A **VMware VC Instance** will now appear in the Storage Manager Devices list. Wait for about 10-15 minutes after completion of the previous step in order to license your ESX Hosts.

Removing VMware ESX Hosts

Complete the following procedure to remove ESX Hosts from a poller.

1. Under Settings in the navigation menu. Click on **Virtualization (Assign ESX Hosts)**

2. On the Assign ESX Hosts page:

a. Select the ESX Hosts you want to remove and use the up arrow button to move them back to the Available list

b. Click **Save**. A push will be scheduled immediately to update the agent(s) with the changes.

Note:

- Clusters can also be assigned in the same manner by selecting 'Cluster' instead of ESX in the ESX Host Assignment page
- If after selecting the Assign by 'Cluster' option, the user clicks on the Save button without actually making any changes, then the ESX hosts which are assigned to a different poller will be re-assigned under the cluster poller.
- If this happens then, you need to re-assign the ESX hosts to its original poller through the 'Assign ESX Hosts' page, by selecting the Assign by 'ESX' option.

VMware vCenter can be defined and assigned to an OS Agent after an OS Agent has been installed and registered with the STM Server. VMware vCenter can discover the ESX Servers connected to Virtual Center.

Important Note: To create a VMware vCenter, make sure that a STM Agent is running on the IP Address you want to use to gather data from.

Application Monitoring

The following sections detail how to configure devices for application monitoring.

MS Exchange 2003/2007

MS Exchange 2003 Clustering

MS Exchange Requirements

Oracle Device

Gathering Exchange 2003/2007 Storage Data

Note: Only roles on one server are supported. Clustering is only supported with Exchange 2003.

STM gathers Storage Groups and Information Store sizes. Below are the requirements for agents to successfully gather this storage information:

- Exchange Services should be running on the Exchange server where STM Agent is installed.
- STM Agent Service should be run using an account that has the required permissions as described below. The Service shouldn't be run using the Local System Account unless this account has all the required permissions.
- This user should have one of the following privileges:

  a. Domain Admin access with Exchange Service permissions and Local Admin permissions.

  b. Permissions are to be applied within the Exchange Organization as ADSI also comes under exchange org.

To be specific, permissions are given to a particular user who has domain account in the exchange organization, who is also the user of ADSI

Exchange 2003 Clustering:

If the STM agent is being setup on a Exchange Active-Passive cluster, follow these steps to set up the agent:

A new configuration parameter for Exchange Clustering has been added in the wrench page of Exchange device

1. Change the value of Exchange Cluster to True
2. Enter the name of the exchange virtual cluster server name in the Exchange Virtual Name field
3. Save the configuration parameters

4. When Exchange data gathering occurs at the next scheduled time, exchange module will start collecting data from the server name entered in the Exchange Virtual Name field.
5. To verify that it is working correctly, run the following commands from the Exchange module directory `- >> ExchangeDataGathering.exe -servername=<virtual name> -storage`

Requirements for Gathering Exchange 2003/2007 Mailbox/Attachment Analysis Data

In addition to the steps above, few additional steps have to be followed to gather Mailbox and Attachments data from Exchange Server 2003/Exchange 2007.

Below are the requirements for the agent to successfully gather Mailbox/Attachments information:

a. The user account that the STM Agent service is running as should be logged on locally to the desktop for setting the MAPI Profile.
b. The User should also have a mailbox setup on this Exchange Server with permissions to access all the other mailboxes (to collect storage data).
c. The user should have a MAPI profile setup on the Exchange server. If not, STM agent ships with a utility called MAPIProfilerTool.exe located in the mod.sys.app.mail.Mail_1.0 module directory. This tool helps the users create a MAPI Profile.
d. Save the attached exe to a temporary folder. Then at the command prompt, run the following: `>>MAPIProfileTool -servername=<Exchange Server ip or host name>`
e. This will bring up a dialog box that says 'Choose Profile'. There will be two alternatives:

If there is a profile already created for the user, then the user can select that from the drop-down.

1. After the user selects a profile, there is a button called 'Options' that brings up two options at the bottom of the dialog box.
2. Check the "Set as default profile" option and click on finish. We need a default profile to be available for the user to log in.
3. ***If there is no profile created for the user, then it will bring up a dialog box asking the user to create one***.
4. You can leave the Profile name that comes up (which is usually MS Exchange Settings).
5. Enter name of the Exchange server and then click **Next**.
6. Choose the default Exchange services

7. Click **Finish.**

This will allow the exe to log in and collect storage data.

Adding an Oracle Device

The STM Server has the capability of monitoring database servers directly via an integrated database performance and usage poller. This function is done without the need of any agents.

Requirements

The following items are required before you begin:

- The STM Server can monitor Oracle 7.2 and above
- The login used when creating an Oracle device should at least have read-only permissions to the V$ tables/views .
- Beginning with version 4.8.6, the Oracle JDBC driver ojdbc.jar is no longer packaged with the STM Server installation. If you wish to add the **"Application Oracle"** Device for monitoring and reporting an Oracle Database, follow the procedure below to download. The driver should be downloaded and installed before you configure the "Oracle Database" Device in STM.

Procedure:

Download the Oracle JDBC driver "ojdbc14.jar" from the following location on the Oracle website:

http://www.oracle.com/technetwork/indexes/downloads/index.html

1. Stop the STM Server "Poller" service

2. Copy the ojdbc14.jar to server install path \webapps\ROOT\WEB-INF\lib

Windows:

Modify <server install path>\webapps\ROOT\bin\Poller.ini and add this string to the second to last parameter (usually 15 or 16) in the end: .\WEB-INF\lib\ojdbc14.jar;

For example:

Before:

- param16 = ..\WEB-INF\lib\profiler-poller-4.9.2.jar;..\WEB-INF\lib\profiler-commons-4.9.2.jar; [shortened for example]..\..\..\common\lib\profiler-jni-4.9.2.jar;

After:

- param16 = ..\WEB-INF\lib\profiler-poller-4.9.2.jar;..\WEB-INF\lib\profiler-commons-4.9.2.jar; [shortened for example]..\..\..\common\lib\profiler-jni-4.9.2.jar;..\WEB-INF\lib\ojdbc14.jar;

Linux / Solaris installation:

1. Modify <server install path>\bin\poller.sh and add this string to the end of the CLASSPATH: :..\WEB-INF\lib\ojdbc14.jar

For example:

Before:

- CLASSPATH="../WEB-INF/lib/profiler-poller-4.9.3-SNAPSHOT.jar: [shortened for example] :../../../common/lib/profiler-jni-4.9.3-SNAPSHOT.jar"

After:

- CLASSPATH="../WEB-INF/lib/profiler-poller-4.9.3-SNAPSHOT.jar: [shortened for example] :../../../common/lib/profiler-jni-4.9.3-SNAPSHOT.jar:..\WEB-INF\lib\ojdbc14.jar"

2. Start the STM Server Poller service.

3. **Go to Settings> All Devices>** to configure the **Application Oracle** Device to set up the Oracle database within STM.

Configuring an Oracle Device

To Configure an Oracle Device:

On the New Device page, provide the appropriate values for the following fields:

- **Server IP Address:** Type the IP Address of the machine where the Oracle server is running
- **Device Display Name:** Type a descriptive name for the Oracle device (ex: Oracle NY1)
- **Oracle Database Name:** Type the Oracle database instance (SID) that you want to monitor
- **Oracle Login Name*:** Type the Oracle user login. This user login should be able to query the system and V$ tables
- **Oracle Login Password***: Type the password for the specified user.
- **Active**: Do not clear this check box, doing so will stop information collection from the device
- **Device Groups**: Optional - if you have configured groups, you can add this device to them by clicking the group name

- **Licensing**: Check this box in order to assign a STM Right To Use (RTU) license to the Oracle device. If you don't check this box, the device will be ignored for data collection

Click **Save** to save the configuration and push it out to the agent to begin monitoring the device.

Editing an Oracle Configuration

To edit an Oracle configuration:

1. **Go to Settings> All Devices>** Filter **Oracle** to display all added devices.

2. Click the wrench icon for the appropriate Oracle device. A configuration page will appear which can be edited.

3. Click **Save** to save the configuration and push it out to the agent and begin monitoring the device.

To Delete an Oracle Configuration:

1. To remove an Oracle device from being monitored, go to the Devices page **Settings > All Devices** and click the delete icon of the Oracle device you want to delete.

2. Click **OK** to confirm deletion.

Note: When you delete an Oracle configuration, you will lose the history.

Chapter 8

Reports and Schedules

STM has the ability to email or print either the Main Console screen or individual device Console information. The printer and letter icons will appear in the upper right hand corner of the screen when this feature is available.

- Click the printer icon to print the console.
- Click the letter icon to email the console information.

STM supports a versatile reporting feature providing summary, inventory and historical information about network performance, storage and devices. The reports provide information about servers, databases, backup operations, NAS and SAN devices. STM provides two levels of reports:

- Manage Reports
- Report Scheduler
- Create A New Report
- Enterprise Report

Administrator Reports

STM is configured with two report options available to administrators and those users with specific permissions only. These options provide instantaneous access to assets, operating systems, storage, and backup statistics across the entire network. When an administrator logs in to STM, two additional selections are available under the Reports menu option.

- **Management Reports:** This selection provides a quick high-level summary of the current network assets, storage and backup.
- **Enterprise Reports:** This selection presents high-level summary views of network performance, while allowing the administrator to drill down to see underlying data. The administrator can look across the enterprise and see a summary view of how much storage space each user is utilizing, then drill down to see the types of files and their locations for that individual user.

Click the Reports folders to expand the report options. The STM user report options are listed below.

- My Reports - Reports you have created
- Shared Reports - Reports other users have created and shared with you

- Quick Reports - Predefined reports

STM uses a consistent format to display and manage reports regardless of which option is selected. Select an option and a table will appear listing the reports available under that option. If no reports are available an error message will be displayed. Within each section, managing reports works the same. You create, run, schedule, modify and delete reports the same way. **Note:** You cannot modify or delete quick reports.

User Reports

STM allows each user to run preformatted and user-defined reports. Both types of reports may be scheduled to run periodically at specific times. The Reports menu selection has several options:

- **My Reports:** This option is for building user-defined reports. These reports will always be accessible to the individual user or the administrator. The user has the option to set the permission level of a report so that the report can be shared with other users.
- **Shared Reports:** Reports created by any user in My Reports may be shared with other users in the same group or with all users. If any reports are shared they will be listed under this menu option. Administrators always have access to all reports, regardless of who created the report.
- **Quick Reports:** This is a selection of reports preformatted by STM. These reports cover a broad spectrum of file, device, and network parameters. Parameters include: disk usage, disk performance, disk and file system inventory, CPU/Memory performance statistics, network statistics and virtual memory performance statistics.

Ability to "**Star**" a report as favorite, is added to My Reports, Quick Reports, and Shared Reports page. A checkbox is added to the top of each page so that the user can filter each page to only show the favorites.

Managing Reports

STM allows for users to schedule reports.

The following steps detail how to run, schedule, create or modify a report

1. Click the **Reports**
2. Select **My Reports, Shared Reports** or **Quick Reports.**

Running a Report

The Action column contains icons indicating the action the user has permission to perform. Possible Action selections include:

Selecting the My Reports option will allow the user to Edit, Delete, Schedule and Run any reports created by that user. A user may also Schedule or Run any report available when the Shared Reports or Quick Reports options are selected.

(**Note:** Administrators always have full access to user-defined reports.) Reports listed under the Quick Reports option are preformatted by STM and cannot be edited or deleted by users or administrators. To take an action, click the icon next to the report you want to run, schedule, modify or delete.

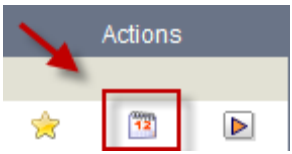
To run a report, simply click the arrow . A Run Report screen will appear with multiple drop-down menus for selecting the scope and output format.

Note: You can only see devices that are in the same groups as you. The Groups drop-down is limited to the groups that you are a member of, and the Devices drop-down is limited to the devices within those groups.

Report Scheduler

To schedule a report:

1. Click the **Schedule icon** in the Report List.



2. This action will show a list of available schedules and the reports assigned to each schedule. You can also schedule reports directly from the Schedule List page.
3. Create a new schedule to assign this report to by clicking the New Schedule icon. This will take you to the Create Schedule page.
4. To assign this report to an existing schedule, click the Add icon for that schedule. This brings up the Create Scheduled Report page.
5. To create or edit a schedule, choose the frequency and time of day you want the report to run.

Summary of options:

- Frequency: Daily, Weekly (pick one or more days), or Monthly (choose the 1st, 15th or the Last Day of the Month)
- Time To Run: The time at which to execute the Report
- Recipients: Select the users who will be notified when this report is run. The users listed are STM users. You can add external email addresses as well.
- Reports: Scheduled Reports assigned to this Schedule

- Publish: How you want to publish the report when it is executed.
- Email Report - send the report in an email to all recipients
- Publish Report (Overwrite) - outputs to the same file name every time report is executed
- Publish Report (Do Not Overwrite) - outputs to a file name plus a time stamp each time the report is executed
- Email: Choose whether all reports should be sent in one email, or broken up into individual emails.
- Name: The name of the schedule

Note: Published reports can be redirected to another location like Sharepoint, UNC etc, with the ‚Target' option available in the Edit Schedule page. For this users must have full access to the share to which the reports are to be redirected to. **You must provide an email address to publish to a share.**

Report Schedule List

Clicking on the Report Schedules icon under the Reports folder in the Tree Menu brings up the Report Schedules List page.

Here you can see a list of all schedules, what reports are assigned to each schedule, the schedule frequency and the next run time.

Exporting Report Data

You can export the data from the report in several ways.

- Email the report in HTML format.
- CSV output, with the following additional choices.

When the second browser window opens, the report has the following features:

- Click a column header to sort
- Click a chart icon to chart that column
- The header will scroll up and down with you
- Totals at the bottom for that page
- Pagination for multiple pages of data
- The ability to email the report
- The ability to close the report

Note: Remember, users can only see devices that are in the same groups as the user. If a user is restricted to just Windows devices then the Enterprise reports visible to the user will contain information about Windows only, not Solaris. If there is no data for the report or the user does not have the permissions to see available data, the report will show:**'There is no data for this report'.**

Enterprise Storage Reports

Enterprise Reports present high-level summary views of network performance, while allowing the administrator to drill down to see underlying data. The administrator can look across the enterprise and see a summary view of how much storage space each user is utilizing, then drill down to see the types of files and their locations for that individual user.

Creating a New Report

To create a new report, click through the menu tree down to **My Reports.** If you have not previously built a custom report, the message **'There are no reports available'** will appear on the screen.

To build a new custom report:

1. Click the **New Report.**
   a. To edit an existing custom report, click the **edit icon.**
2. Choose the Scope of your report.

For example, if you choose Enterprise, you will be able to run reports that apply to all devices across the enterprise. If you choose Windows, you can only run Windows specific reports.

3. Select **Report Type**. The report type defines the types of data you want to report.
4. Click **Continue.**
5. Select the fields you want for your report.
6. Click the **Continue**.
7. Select the sorting, filtering and permission structures for this report.

Structure Scenarios to consider:

You may sort according to any chosen statistic in ascending or descending order. Once the report is executed, you can dynamically change the sort.

Filters allow you to include or exclude statistics based on standard filter criteria (like, not like, >, >=, etc.). You can apply more than one filter to a query.

Rows per page set the default rows per page for this report. Permissions options include myself (only I can run the report), Group (all users in the groups I am a member of), or All (all users).

8. Click **Continue.**
9. Enter a name for the report.
10. Click **Save**. The report will appear on the My Reports list.

Deleting a Report

To delete a report, click the Delete icon (trash-can) to the right of the report name in a reports list.

If you click the Delete icon, a message will appear asking you to confirm your selection. To delete the report, click the **OK.**

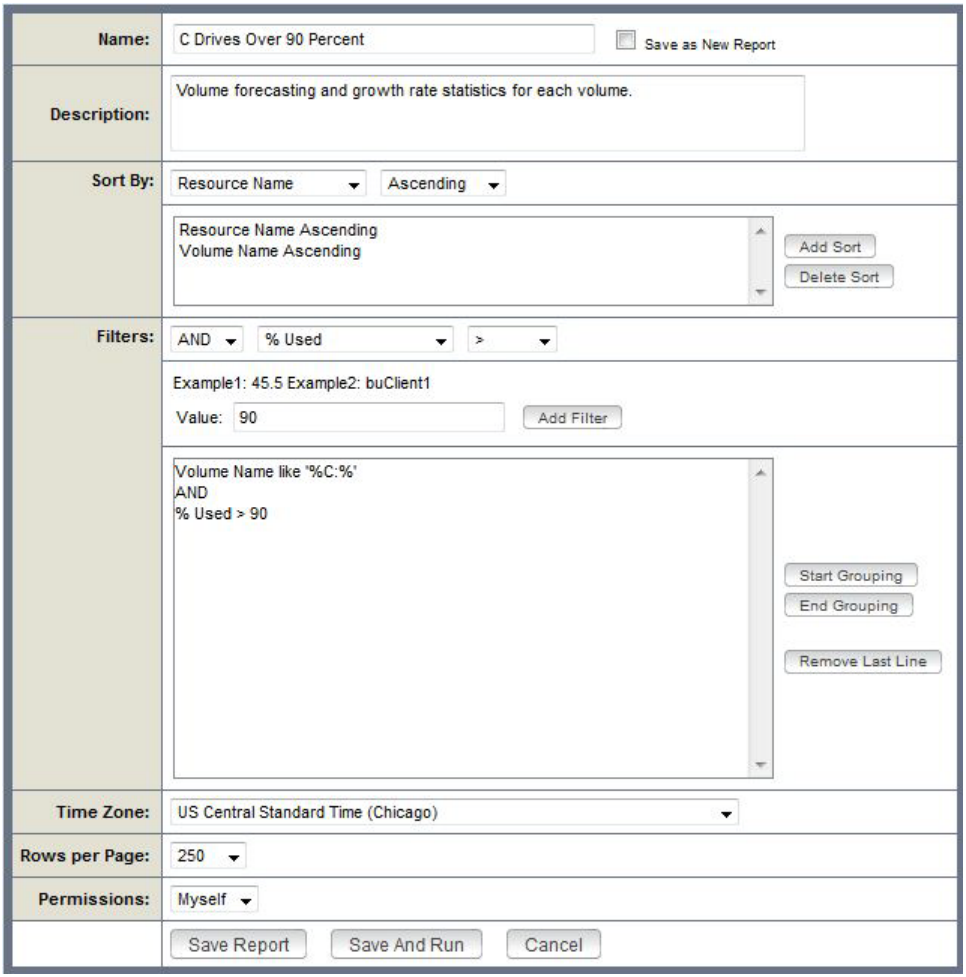
Note: You will neither be able to delete a Shared Report that you have access to, nor a Quick Report.

Example Report

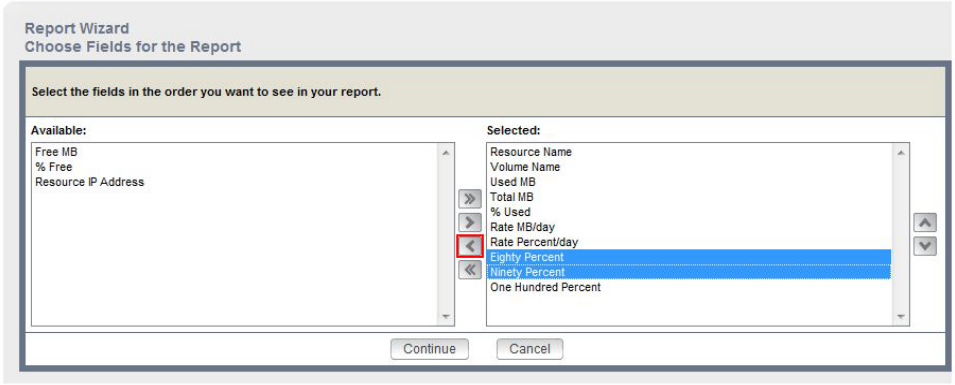
When you build a custom report, you are simply selecting the fields you want to see, in the order you want to see them, and adding filters to narrow the results. At report execution (either on-demand or scheduled), you will be able to select the set of devices, the time period, and other variables, in order to narrow the results further.

For example, assume you wanted to find all the servers in your environment where the C:\ drive was greater than 90% full, and you want to understand how fast they are growing. We have the template **"Volume Usage Forecast"** we can leverage as a starting point**. Go to Reports > My Reports** and click the **New Report** button, and then select the template you want to use.

Select **Enterprise > Storage > Volume Usage Forecast** and then click **Continue:**

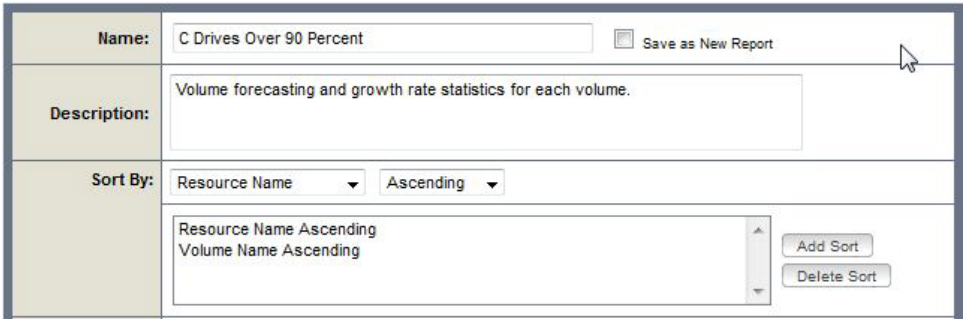


Next, select the columns you want in the report and the order of those columns. Each template has defaults for the columns selected, the column order and the sort order. Remove the Eighty and Ninety percent columns by highlighting them and clicking the left arrow.



Next, select the sorts and filters for the report, allowing us to narrow the output to exactly what we want.

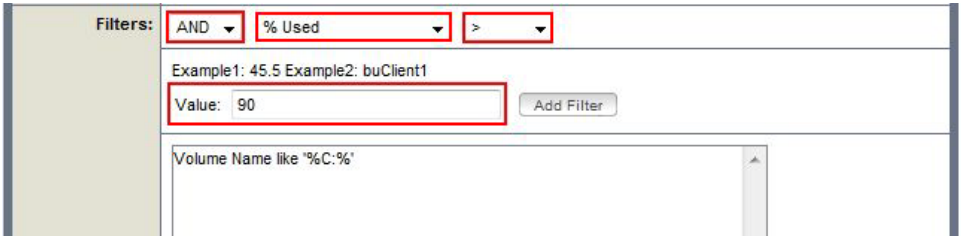
Enter the name of the report "C Drives Over 90 Percent" and in this case, you will leave the default sort (server, volume) in place. If you wanted to change the sort order, you can remove current sorts by highlighting them in the text box and clicking **Delete Sort,** and add new sorts by selecting the **Sort By** field and order by clicking "**Add Sort".** The order of the fields in text box is the order the sort will be applied to the report.



Next, you will pick the filters. In general, you can filter by any column in the report, and the options of the filter will match the data type:

- Text Fields: like, not like, <, >, =, <=, >=, <>, in, not in
- Numeric Fields: like, not like, <, >, =, <=, >=, <>, in, not in
- Date Fields: <, >, =, <=, >=, <>, before, within

The basic query you will build is "*Volume Name like C: AND % Used > 90*". So for the first part select "**Volume Name**" and "**like**" and enter "*%C:%"* and then click "**Add Filter**" - you should see the filter appear in the text box. For "**like**" filters, make sure you add the "**%**" before and after the text. **Note:** Since this is the first filter, you can ignore AND/OR drop down.



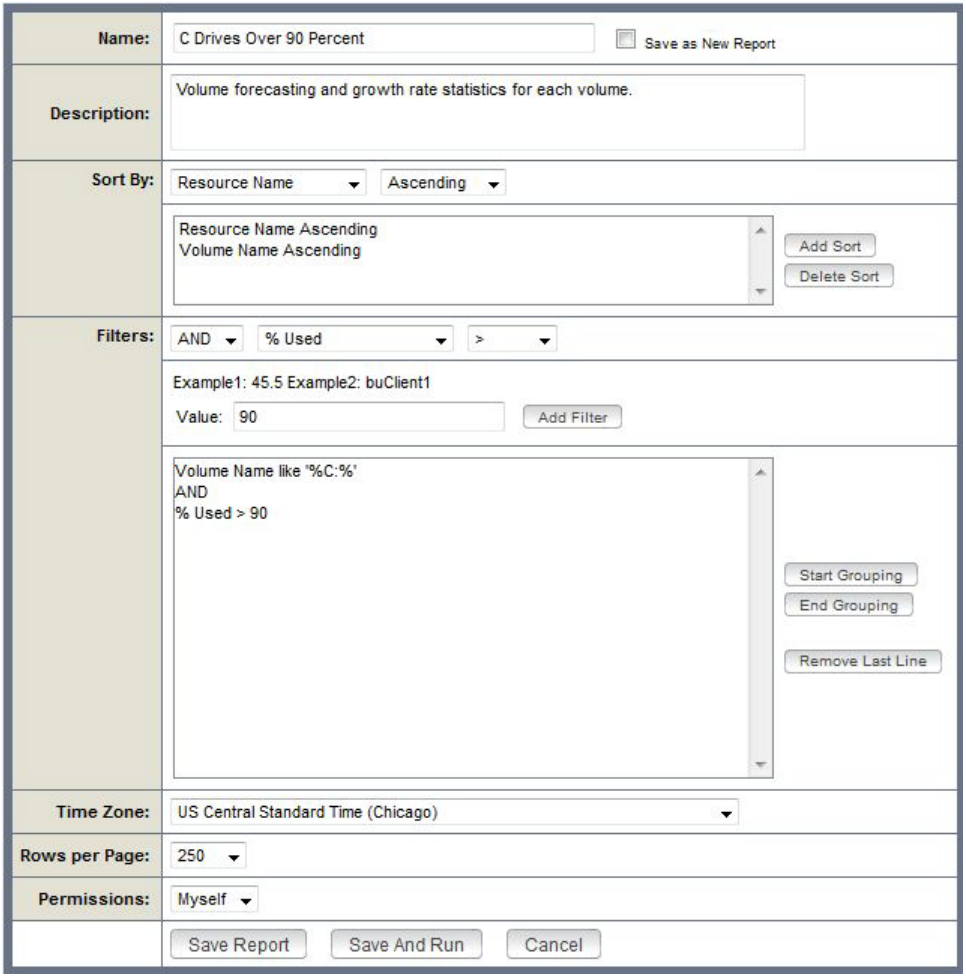
For the second filer, choose "*AND", "% Used", " > "* and enter "*90*" and click "**Add Filter**".

Filters:
AND
Volume Name
like
Example: Windows Host
% - Matches zero to any number of characters (\% to search for % character)
_ - Matches exactly one character (_ to search for _ character)
Value: %C:%
Add Filter

Finally, there are few additional items to select:

- **Time Zone**: The default time zone of the report, which can be changed at run time.
- **Row per Page:** The default rows per page.
- **Permissions:** What users can see this report: **Myself**, **Group** (All users in my groups), **All** (everyone).

Now save the report and your page should look like this.



Available actions:

- **Save Report** - saves the report and returns to My Reports.
- **Save and Run** - saves the report and takes you to the Run Report page
- **Cancel** - abort changes to the report and return to the My Reports list.

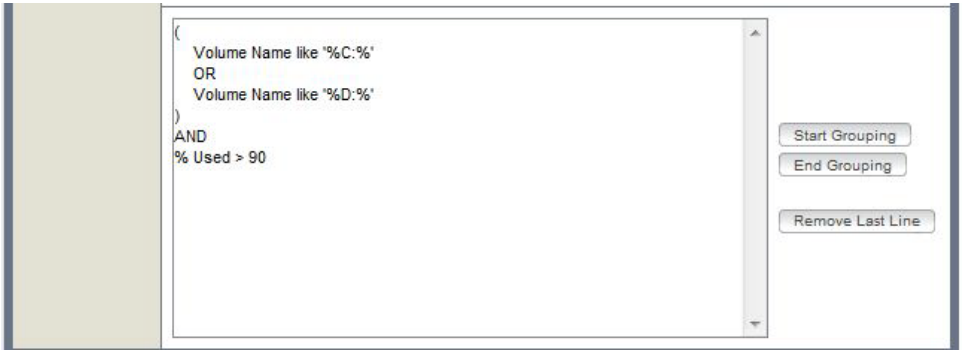
For this report, if you select **Save and Run**, and then run the report, the output looks like this (assuming you have some C:\ drives over 90%).

C Drives Over 90 Percent

Show Description
Enterprise: Volume Usage Forecast
Printer Friendly

Row	Resource Name	Volume Name	Used MB	Total MB	% Used	Rate MB/day	Rate Percent/day	One Hundred Percent
1	cd-fin-web	C:\	65,475.89	69,965.61	93.58	<0.01	<0.01	2+ years
2	chiappd01	C:\	14,698.75	15,351.14	95.75	1.96	0.01	Mar 23, 2011
3	chiqmmp01	C:\	28,053.75	30,710.16	91.35	5.00	0.02	Oct 9, 2011
4	chispsd27-a	C:\	14,902.52	15,351.11	97.08	20.91	0.14	Already reached
5	chisqlp06	C:\	14,147.23	15,351.11	92.16	16.68	0.11	Already reached
6	chisqlt01	C:\	13,927.45	15,351.14	90.73	1.12	<0.01	2+ years

You have the ability to group filters, so you can do "Find all (C: OR D:) drives that are over 90%".



So that is how you build a custom report - it is quite flexible and lets you get to your data exactly how you want it.

Here are some ways users can leverage the reporter functionality:

- Identify problem areas before they become "problems" - busiest LUNs, fullest drives, busiest VM or ESX, etc.
- Chargeback - charge users, departments, customers, etc. for the storage, backups or servers they are using.
- Backup Compliance - identify full backups that have not been successful for more than 7 days.
- User Quotas - identify users exceeding their storage quota

Using Groups

The Grouping functionality allows an administrator to define a logical organization and permission structure to the data that is gathered by STM. A Group console can quickly show an overview of its devices as a whole, and serve as a quick link to those devices.

Grouping also determines the permissions for what a user can see. Users can only see devices with the same group(s) permissions.

Groups are completely user-defined, and can be used to represent departments, projects, server types, and lines of business, operator assignments or any other category that is relevant to your specific organization. When you are assigning devices, objects and users to groups, it affects STM's interface in the following ways:

Tree Menu: (The structure of the tree menu) Only the groups and devices the user has permissions will appear in the tree menu.

Reports: The groups available when a report is executed or scheduled: Only the groups and devices the user has access will be available.

Consoles: Console can quickly show an overview of its devices as a whole, and serve as a quick link to those devices.

When you define a group, you can put different types of objects in them, including:

- Backup Servers
- Backup Clients
- Databases
- Email
- OS Devices
- Volumes (File Systems)
- Shares
- Storage Systems (EMC, NetApp, Xiotech)
- Fibre Channel Switches and Ports
- LUNs & Qtrees
- VMware VMs & ESX
- Users

One way to think of a group is as a bucket. You place all the objects that logically belong together into a single bucket and STM will sort them into categories and determine permissions. The default categories that STM sorts these objects into are:

- Backup Servers
- Backup Clients
- Database Servers
- Email Servers
- Devices (all OS and NAS Devices)
- SAN devices (all supported Storage Arrays, Generic SAN Arrays, and Fibre Channel Devices)
- Storage Groups (File Systems and Shares)
- Fibre Channel Ports
- LUNs & Qtrees
- VMware VMs & ESX

If a category does not have any objects, then that group will not be represented in the tree menu.

For backup clients, STM also allows subgroups. This function allows a user to group backup clients into logical groups and subgroups, even if those clients are backed up by different servers. Backup clients may be monitored or unmonitored devices.

You may also assign an accounting code to each group. This function will allow you to see the accounting code in some management reports.

Important Notes:

- Devices may belong to multiple groups. For example, all NT servers to be assigned to the group, "All NT Servers" and, at the same time, some of those NT servers could also be grouped as "Finance" while others are grouped as "Sales."
- When you put a device into a group, it does not automatically add the file systems to the group. You must assign each file system individually. File systems can only be assigned to one group.
- Subgroups are used for backup clients only.

- When creating a device, if you do not associate it with a group you have defined, and then it will be associated with the default group Unassigned. Once you have associated a device with at least one group, the association with the unassigned group is dropped.
- Only a user with administrator privileges can see the "Unassigned" group.

Managing Groups

To access the Groups function from the left navigation tree:

1. Click the **Groups** option in the drop-down menu that appears under the Administration folder of the STM tree menu at the left side of the screen.

The Groups screen will appear, listing all groups previously created.

Note: subgroups appear indented.

From this screen you can create, edit and delete your groups and subgroups.

To create a new group:

1. Click **Add Group** and go to the Creating Groups section.

To create a new subgroup:

1. Click **Add Sub Group** and go to the Creating Groups section.

To edit a group, click the edit icon next to group you want to edit. The screen that appears is identical to the Create New Group screen, except you will be not be able to edit the group name.

To delete a group, click the trash icon next to the group you want to delete. Note that all associations with devices and users are deleted when you delete a group. If a device is not associated with any other group than the one you are deleting, it will be associated with the default Unassigned group.

Creating Groups

To create a new group

1. Click **Add Group** on the Groups screen.
2. Type the name of the new group in the **Group Name field**.
3. Select from the available categories.

Summary of Categories:

- **Backup Server:** All backup servers. Backup Servers can belong to multiple groups.

- **Backup Client:** All backup clients, including monitored and unmonitored devices (a monitored device has an agent, an unmonitored device does not), not assigned to another group. Backup Clients can belong to multiple groups.
- **Database:** This function allows you to group databases into logical groups for monitoring.
- **Email:** This function allows you to group email servers into logical groups for monitoring.
- **Quantum:** This function allows you to group Quantum devices into logical groups for monitoring.
- **Servers & NAS**: All OS and NAS devices defined on the Devices page. A device can belong to one or more groups.
- **Storage** - **Volume:** All volumes (file systems) from all OS and NAS devices not assigned to another group. This allows you to associate volumes into logical collections of storage independent of the device it resides (Note each volume in the assignment window shows the device name and volume name). This allows for easy chargeback reports as they show storage allocation and usage summaries per group. These groups are also used in the Management reports to show allocated and used space per group. Volumes & file systems can be assigned to more than one group.
- **Storage - Share**: This function allows you to group shares into logical groups for monitoring.
- **User:** All the users defined in STM. Administrators are always a member of every group. This function is done in the background automatically. If you remove an administrator from a group and then save it, STM will add it back automatically. Users can belong to one or more groups.
- **Storage - Qtree** This function allows you to group Storage Qtrees into logical groups for monitoring and chargeback.
- **SAN Switch - Ports:** This function allows you to group SAN Switch Ports into logical groups for monitoring.
- **Storage - LUN** This function allows you to group Storage LUNs into logical groups for monitoring and chargeback.
- **VMware VM** This function allows you to group VMware VMs into logical groups for monitoring.
- **VMware ESX** This function allows you to group VMware ESX into logical groups for monitoring.

Note: User will have access only to the file system/shares/Qtrees in the group assigned to him.

4. To save the new group click the '**Save'.** The group list will reappear with the new group in the list.
5. To cancel creation of the new group, click the **Cancel.** The group list will reappear.
6. To assign an object to a group, click the object in the **Available** box and click the down arrow and it will move the object to the **Selected** box (and vice versa).

To assign multiple objects:

7. CTRL-click multiple objects in the **Available box**. The double arrows will move all Available objects into the selected box (and vice versa).

If your lists of objects are long, you can filter for the items you want to find by using the **Filter by Regular Expression box.**

You can filter by the beginning letter by clicking it, or you can enter you own regular expression to find the object you are looking for.

Creating Subgroups

STM has a special ability to create subgroups for backup clients. This ability allows you to put backup clients into logical groups even if they are backed up by more than one server.

Note: There are only two levels of groups for backup clients.

To create a new subgroup:

1. Click Add Sub Groups on the Groups screen.
2. Choose the super group for this subgroup.

Note: A subgroup cannot be a super group. Enter a name for the subgroup.

3. To assign a backup client to the group, select backup clients on Available box and click it will move to the "Selected" box. To remove a backup client from a group, select backup clients on "Selected" box and click it will move to the Available box. Same applies for the Users section.
4. To save the new subgroup click **Save,** the group list will reappear with the new group in the list.
5. To cancel creation of the new subgroup, click **Cancel.** The group list will reappear.

File Type Groups Page

The File Type Grouping functionality allows an administrator to define a logical organized structure to the data that is gathered by STM.

The File Type Groups Page displays the existing File Type Group Names.

To edit a File Type Group click the edit icon from the File Type Group list. The same console and functions as in 'Add File Type Group' will appear. To delete a File Type Group click the Delete icon from the File Type Group list.

Creating File Type Groups

1. Click **Add** to add a new Group. The 'Create New Group' console will appear.

   Group Name: Enter the name of the group.

   Case-sensitive: Define whether the file names will be case-sensitive. If the box is checked, file names with capital letters will be different than names with lower case letters.

   File Types: A list of file types (extensions) returned by the console. The files can be selected by using filters based on starting letters, expression, or by adding a new file type.

2. Once the file types have been selected from the available area, click to add them to the selected list.
3. Click **Save**. The File Type Group list will reappear with the new group in the list.

Chapter 9

Rules & Policies

The follwing section details the various rules you can create to achieve certain actions. Once you have created a rule you can then apply them to a policy.

- Rules
- Policies

The types of rules the user can create.

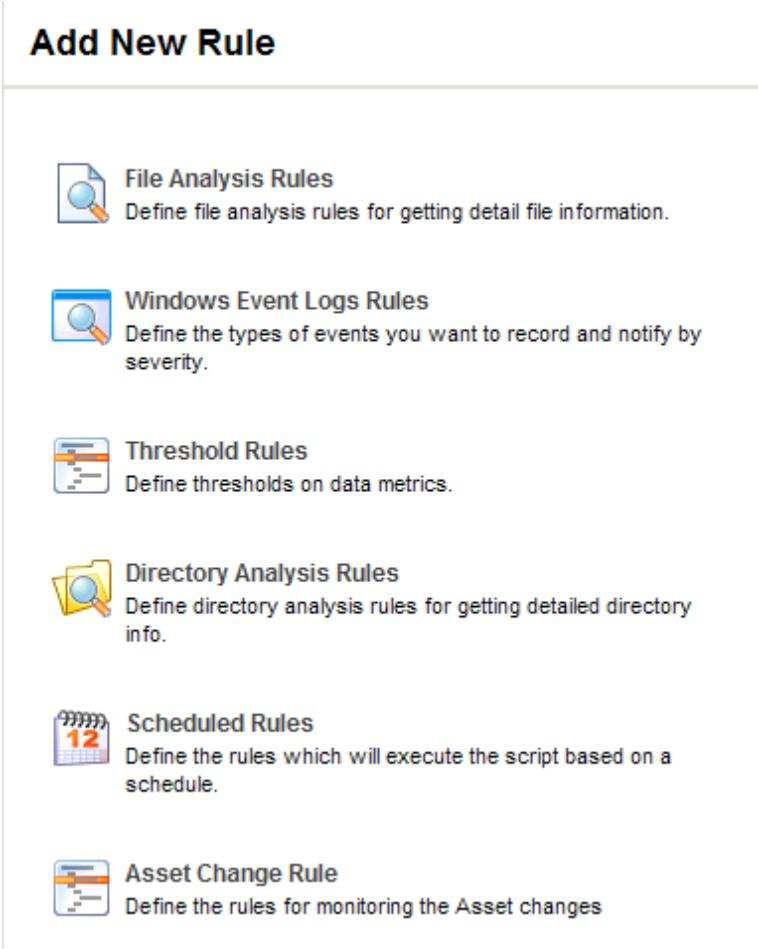
- File Analysis Rules
- File Analysis on NAS and Virtual Machines
- Defining Threshold Rules
- Windows Event Logs Rules
- Directory Analysis Rules
- Scheduled Rules

- Snap Mirror Monitoring

The following section details how to create new rules.

To create a new rule:

1. Click **Settings** in the left navigation menu.
2. Click **Rules.**
3. Click **Add New Rule.**
4. Select from one of the following:


Add New Rule
File Analysis Rules
Define file analysis rules for getting detail file information.
Windows Event Logs Rules
Define the types of events you want to record and notify by severity.
Threshold Rules
Define thresholds on data metrics.
Directory Analysis Rules
Define directory analysis rules for getting detailed directory info.
Scheduled Rules
Define the rules which will execute the script based on a schedule.
Asset Change Rule
Define the rules for monitoring the Asset changes

5. Enter the necessary information and then click **Save**

File Analysis Rule

The File Analysis Rule lets you define rules that will provide detailed file information.

STM currently limits the number of files returned to 5000 per target. You can subdivide the current target by doing local or remote shares, leveraging the **depth** function, which automatically subdivides the target per subdirectory.

What is File Analysis?

- Analyzes how you are using your file storage
- Works on any formatted storage: Server, VM or NAS device

What does it report?

- Summary Information
- By Owner, Age and Type
- Find specific files via File Rules
- File Information - Size, owner, access, creation, modification

These rules are applied to devices via the **Policies** menu under **Settings.**

- **Rule Name:** Enter the name of the rule.
- **Find the X Y files with:** X represents the max number of files reported on. It is on a per file system/share basis. Y represents the limit type to be used in cases where more than max(X) number of files are found. The choices are largest, oldest accessed and oldest modified.
- **Size:** If you leave the value set at 0, then all files will be evaluated, and considered potentially valid, regardless of size. Otherwise, only files that are at least the selected size (specified in megabytes) will be evaluated and considered potentially valid.
- **Accessed Age:** If you leave the value set at 0, then all files will be evaluated, and considered potentially valid, regardless of access time. Otherwise, only files that are at least this age, in regards to access time, will be evaluated and considered potentially valid.
- **Modified Age:** If you leave the value set at 0, then all files will be evaluated, and considered potentially valid, regardless of modified time. Otherwise, only files that are at least this age, in regards to modified time, will be evaluated and considered potentially valid.

- **Created Age:** If you leave the value set at 0, then all files will be evaluated, and considered potentially valid, regardless of created time. Otherwise, only files that are at least this age, in regards to created time, will be evaluated and considered potentially valid.
- **File Path Regular Expression:** You can specify a regular expression (based on the Java implementation of regular expressions) that all files must match, in regards to file name and path, in order to be evaluated and considered potentially valid. If nothing is specified, then all files are evaluated, and considered potentially valid.
- **Regex Examples:**

    1. **To Find files that have a date in their extension, e.g. 2006-09-20 :**
       Create a Rule with the File Path Regular Expression ***.*[\d]{4}-[\d]{2}-[\d]{2}.**** This returns files like "Localdevice_log.2007-09-04.txt" as well as files like "bookmarks-2007-10-01.html".

    2. **To Find only log files that have a date in their extension:**
       Edit the File Path Regular Expression in (1) to ***.*log.[\d]{4}-[\d]{2}-[\d]{2}.**** This will give just the log files with a date in the file name.

    3. **To modify the search in (2) to exclude years ending in 6 e.g. 2006**
       Edit the File Path Regular Expression to ***.*log.[\d]{3}[0-5[7-9]]-[\d]{2}-[\d]{2}.****

    4. **To Find files with extensions line ab5e1073_ad9b_48df_b07f_3e445b5a45cf.**
       Create a Rule with the File Path Regular Expression ***.*[\w]{8}_[\w]{4}_[\w]{4}_[\w]{4}_[\w]{12}.****

    5. **To Find files that start with the numbers 118:**
       Create a Rule with the File Path Regular Expression ***.*118[\d]{7}.****

    6. **Regular expression to exclude all ZIP Files:**
       Create a Rule with the File Path Regular Expression ***.*(?i:(?<!\.zip))$***

    7. **Regular expression to exclude PST and OST files:**
       Create a Rule with the File Path Regular Expression ***.*(?i:(?<!\.[op]st))$***

For documentation on Regular Expressions in Java, refer to
http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html

- **File Types:** A list of file types (extensions) returned by the rule. The files can be selected by using filters based on starting letters, expression, or by adding a new file type.

- **Case-sensitive:** Define whether the file names will be case-sensitive. If the box is checked, file names with capital letters will be different than names with lower case letters.

6. Click **Save.**

Note: To turn on file analysis for a specific server, go to the Devices page (**Settings> Devices)** and click the wrench of the server. On the configuration page that pops up, go to the file analysis section.

Set the Status to “On” and set the Start Time (defaults to midnight). File analysis will run every unless you change the frequency.

File Analysis on NAS and Virtual Machines

The following section describes how to setup file analysis on NAS and Virtual machines and is based on the scenario of determining who has files, what kind of files and how old the files are on each share.

This would allow you to:

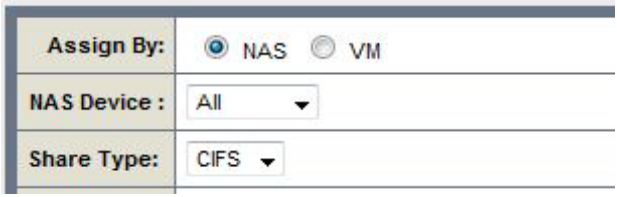
- Obtain size and details on each share
- Used for quota enforcement
- Compliance reporting
- Storage recovery
- You can also group shares into logical collections for chargeback.

Requirements:

- First, we need a list of shares from the device. For NetApp, this is done automatically through the API. For Celerra, Virtual Machines, and other NAS devices, you assign this work to an agent. If you are not seeing a list of shares, then most likely you have a permissions issue. See the FAQ at the bottom for more details.
- An agent that is assigned the work must be able to access the share. For Windows, this means changing the Service Account to a domain user that has access to those CIFS shares. For Unix/Linux, it means the root user should have access to the NFS shares.
- All CIFS scanning is done by agents on Windows servers, and all NFS scanning by agents on Unix/Linux servers.
- You must turn file analysis to "On" on the agent doing the work.

To assign shares for NetApp:

1. Go to Settings > Assign Remote Shares and choose the following (changes in selection will refresh the screen)

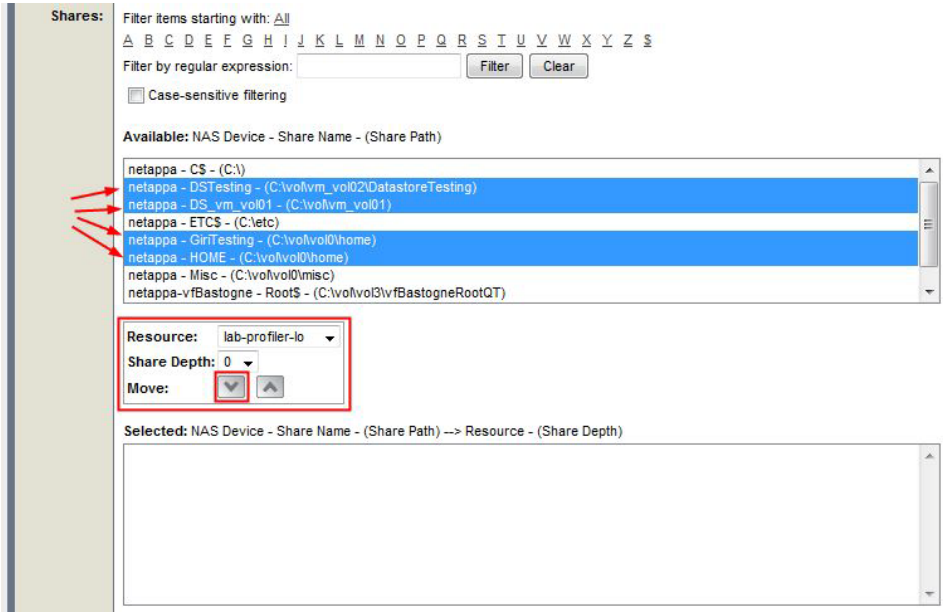


2. Assign By: NAS or VM - lets you choose if you want to see NAS devices or Virtual Machines

   [NAS/VM] Device: Select one device or all devices.

   Share Type: CIFS or NFS. This will automatically change available agent to match the protocol.

3. Once you have set the above criteria, you can then select the shares you want:


Shares:
Filter items starting with: All
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z $
Filter by regular expression:
Filter
Clear
Case-sensitive filtering
Available: NAS Device - Share Name - (Share Path)
netappa - C$ - (C:\)
netappa - DSTesting - (C:\vol\vm_vol02\DatastoreTesting)
netappa - DS_vm_vol01 - (C:\vol\vm_vol01)
netappa - ETC$ - (C:\etc)
netappa - GiriTesting - (C:\vol\vol0\home)
netappa - HOME - (C:\vol\vol0\home)
netappa - Misc - (C:\vol\vol0\misc)
netappa-vfBastogne - Root$ - (C:\vol\vol3\vfBastogneRootQT)
Resource:
lab-profiler-lo
Share Depth:
0
Move:
Selected: NAS Device - Share Name - (Share Path) --> Resource - (Share Depth)

1. You can narrow it down the shares by using the regular expression filter.
   a. Select the shares you want. You can select multiple shares by using the CTRL or SHIFT key.
   b. Now you will select which agent is going to do the work
   c. Device: select which agent you want to do the work
   d. Share Depth: Leave this at zero for now - more on depth later
   e. Move: Press the down arrow to assign the share, up arrow to unassign shares.
2. Once you have assigned the shares to the agents you want, press Save at the bottom. This will immediately assign out the shares to that agent, and file analysis will be performed at the next scheduled file analysis start time for that agent. If you want to change the start time, the previous post Files, Files, Everywhere... shows you how to do that.

Defining Threshold Rules

The Threshold Rule page allows you to set thresholds for conditions and determine if scripts need to be run or SNMP traps sent. The following descriptions detail the available options.

- **Rule Name:** The name you would like to give this rule.
- **Section:** The section of the devices that you would like to monitor. This can be done across the Enterprise or by system type.
- **Category:** The category you would like to monitor.
- **Choose Instances:** The specific instances you like to rule upon. Click on to add them to the selected list.
- **Condition:** The condition you would like to set. First select the field to monitor, then the condition, and then the value to evaluate the condition against.
- **Duration:** The duration that the condition must be true for the action to be taken
- Then select one of the following:
- **Run Client Script:** The script that needs to be run when the condition is met (client-side based).
- **Run Server Script:** The script that needs to be run when the condition is met (server-side based).
- **Send Trap:** Send out SNMP trap.

SnapMirror Monitor

The SnapMirror Monitor shows the current transfer between the source and the destination for all the filers in the group or a particular filer based on the filter selection.

Filtering the view:

- **Groups -** All Groups assigned to the logged in user with NetApp or IBM N Series Filers devices will be displayed
- **Source Filer -** Filers in all the Groups will be displayed. On selection of a particular group, source filer drop down box will be loaded with filers in that groups
- **Status -** Displays the possible statuses that can happen during snap mirror transfer, user can filter based on the selected status by selecting the desired status and clicking on 'GO' button

Sorting the view:

- **Groups** - All Groups assigned to the logged in user with NetApp or IBM N Series Filers devices will be displayed
- **Source Filer -** Filers in all the Groups will be displayed. On selection of a particular group, source filer drop down box will be loaded with filers in that groups
- **Status -** Displays the possible statuses that can happen during snap mirror transfer, user can filter based on the selected status by selecting the desired status and clicking on 'GO' button

Windows Event Log Rule

Windows Event Log Rules allow you to receive alerts whenever an event takes place. Once created, you must 'Push' the policy to begin receiving alerts.

To enable a Windows Event Log Rule:

1. Ensure that Event log monitoring is enabled.
2. Go to **Settings > Rules** and add a new **Windows Event Log** rule.
3. Next, go to **Settings > Policies** and add the rule to the policy that the Windows host(s) belongs to.
    - **Rule Name:** The name of the Windows Event Logs rule.
    - **Event Log:** The log file you wish to monitor (Application, System).
    - **Event Source:** The type of event in the event log you wish to monitor.

- **Event ID:** The event ID you wish to monitor.
- **Record and Notify:** The types of events you would like to either record or be notified on.

Directory Analysis Rule

The Directory Analysis Rules allows you to specify certain criteria for identifying directories. Limit Size which helps you minimize the impact to the database by selecting one of the following limit sizes: 10 / 20 / 50 / 100 / 250 / 500. This will be the limit size per file system/share.

Rule Name: The name you would like to give this rule.

Limit Type: In cases where the result set is larger than the value you selected for limit size, the result set will be trimmed based on one of the following criteria, depending on which one you select:

- Total directory count, including sub-directories (lowest values will be trimmed)
- Total file count, including sub-directories (lowest values will be trimmed)
- Total file size, including sub-directories (lowest values will be trimmed)
- Access age, including sub-directories (latest values will be trimmed, i.e. oldest directories kept)
- Modified age, including sub-directories (latest values will be trimmed, i.e. oldest directories kept)
- Files percentage, including sub-directories (lowest values will be trimmed)
- Total file count, current directory ONLY (lowest values will be trimmed)
- Total file size, current directory ONLY (lowest values will be trimmed)
- Access age, current directory ONLY (latest values will be trimmed, i.e. oldest directories kept)
- Modified age, current directory ONLY (latest values will be trimmed, i.e. oldest directories kept)
- Files percentage, current directory ONLY (lowest values will be trimmed)

Limit Size: In order to minimize the impact to the database, you will be able to select one of the following limit sizes: 10 / 20 / 50 / 100 / 250 / 500. This will be the limit size per file system/share.

Minimum Directory Count: numeric values that you would like to set in order to filter out directories that do not contain at least X number of directories. This count includes sub-directories.

Minimum File Count: numeric values that you would like to set in order to filter out directories that do not contain at least X number of files. This count includes sub-directories.

Minimum Total File Size in MB: A numeric value that you would like to set in order to filter out directories that do not contain at least X number of megabytes of files. This count includes sub-directories.

Minimum Access Age in Days: Numeric values that you would like to set in order to filter out directories that do not contain files that are at least X number of days old in terms of access time. This can be used to find high level directories that have not been accessed in a very long time. This count includes sub-directories.

Minimum Modified Age in Days : A numeric value that you would like to set in order to filter out directories that do not contain files that are at least X number of days old in terms of modified time. This can be used to find high level directories that have not been accessed in a very long time. This count includes sub-directories.

Minimum Total File Size Percentage: Numeric values that you would like to set in order to filter out directories that do not contain files totaling X percent of the parent directory, in terms of size. This count includes sub-directories.

Minimum File Count: Numeric values that you would like to set in order to filter out directories that do not contain at least X number of files. This count is for the current directory only.

Minimum Total File Size in MB: A numeric value that you would like to set in order to filter out directories that do not contain at least X number of megabytes of files. This count is for the current directory only.

Minimum Access Age in Days: Numeric values that you would like to set in order to filter out directories that do not contain files that are at least X number of days old in terms of access time. This can be used to find the exact directories that have not been accessed in a very long time, based on the files they contain. This count is for the current directory only.

Minimum Modified Age in Days: A numeric value that you would like to set in order to filter out directories that do not contain files that are at least X number of days old in terms of modified time. This can be used to find the exact directories that have not been accessed in a very long time, based on the files they contain. This count is for the current directory only.

Minimum Total File Size Percentage: Numeric values that you would like to set in order to filter out directories that do not contain files totaling X percent of the parent directory, in terms of size. This count is for the current directory only.

Directory Path Regular Expression: A regular expression that you can set in order to restrict the directories considered to a subset. For instance, if the user were only trying to find information about directories below “C:\winnt\”, a regular expression could be added to restrict directories considered valid, to be within “C:\winnt\”, ignoring all others. If this option is left blank, all directories will be considered valid.

Report: Generate a report that matches the rule.

Schedule the selected Action: Schedule the action you selected above.

Managing Rules

- Scheduling Rules
- Asset Change Rule

The STM server has the capability of taking actions based on rules.

The Menu will show different sections of types of rules that the user can create.

File Analysis Rules consist of:

- Windows Event Logs Rules
- Threshold Rules
- Directory Analysis Rules
- Scheduled Rules

To define a File Analysis Rule provide the following:

a. **Rule Name:** Enter the name of the rule.

b. **Find the X Y files with:** X represents the max number of files reported on. It is on a per file system/share basis. Y represents the limit type to be used in cases where more than max(X) number of files are found. The choices are largest, oldest accessed and oldest modified.

c. **Size of:** If you leave the value set at 0, then all files will be evaluated, and considered potentially valid, regardless of size. Otherwise, only files that are at least the selected size (specified in megabytes) will be evaluated and considered potentially valid.

d. **Accessed Age:** If you leave the value set at 0, then all files will be evaluated, and considered potentially valid, regardless of access time. Otherwise, only files that are at least this age, in regards to access time, will be evaluated and considered potentially valid.

e. **Modified Age:** If you leave the value set at 0, then all files will be evaluated, and considered potentially valid, regardless of modified time. Otherwise, only files that are at least this age, in regards to modified time, will be evaluated and considered potentially valid.

f. **File Path Regular Expression:** You can specify a regular expression (based on the Java implementation of regular expressions) that all files must match, in regards to file name and path, in order to be evaluated and considered potentially valid. If nothing is specified, then all files are evaluated, and considered potentially valid.

Regex Examples:

- **To find files that has a date in their extension, e.g. 2006-09-20:** Create a Rule with the File Path Regular Expression ***.*[\d]{4}-[\d]{2}-[\d]{2}.**** this returns files like "Localdevice_log.2007-09-04.txt" as well as files like "bookmarks-2007-10-01.html".

- **To Find only log files that has a date in their extension:** Edit the File Path Regular Expression in (1) to ***.*log.[\d]{4}-[\d]{2}-[\d]{2}.**** this will give just the log files with a date in the file name.

- **To modify the search in (2) to exclude years ending in 6 e.g. 2006** Edit the File Path Regular Expression to ***.*log.[\d]{3}[0-5[7-9]]-[\d]{2}-[\d]{2}.****

- **To Find files with extensions line ab5e1073_ad9b_48df_b07f_3e445b5a45cf.** Create a Rule with the File Path Regular Expression ***.*[\w]{8}_[\w]{4}_[\w]{4}_[\w]{4}_[\w]{12}.****

- **To Find files that start with the numbers 118:** Create a Rule with the File Path Regular Expression ***.*118[\d]{7}.****

g. **File Types:** A list of file types (extensions) returned by the rule. The files can be selected by using filters based on starting letters, expression, or by adding a new file type.

h. **Case-sensitive:** Define whether the file names will be case-sensitive. If the box is checked, file names with capital letters will be different than names with lower case letters.

1. Once the file types have been selected from the available area, click to add it to the selected list.
2. Next, the rule can be filtered by file owner.
3. Select from the available owners and click to add it to the selected list.
4. Click **Save.**

Scheduling Rules

The Schedule Rules page lets you execute a script on the device machines at a given schedule.

- **Rule Name:** Enter a name for this rule
- **Script:** From the drop down list, select a script that you want this rule to execute. To add a new script, go to Administration-> Scripts page.
- **Parameters:** If you would like to send any parameters to the script while executing, enter them here.
- **Schedule:** Select the schedule for this rule. The rule will be executed on the device machines according to this schedule.

Asset Change Rule

The Asset Change Rule page lets you execute a script on the device machines when any asset change occurs.

1. Provide the following
   a. Rule Name: The name you would like to give this rule.
   b. Section: The section of the devices that you would like to monitor.
   c. Category: The category you would like to monitor.
   d. Property: The property you would like to select.
2. Select one of the following:
   - **Run Client Script:** The script that needs to be run when the condition is met (client-side based).
   - **Run Server Script:** The script that needs to be run when the condition is met (server-side based).

- **Send Trap:** Send out SNMP trap.

Using External Scripts

The STM Server has the capability to manage external scripts and execute them via the STM Agent. The Scripts page shows the user the current scripts that have been uploaded to the STM Server.

Scripts can be dispatched to STM Agents and executed when a threshold condition is met or on a schedule. See "**Error! Reference source not found.**" page "**Error! Bookmark not defined.**" for more information.

To directly edit a script:

1. Click '**Scripts'** under the Settings menu, a Scripts List screen is displayed.
2. Click the **hyperlink** in the File Name column to directly edit the contents of the uploaded script.
3. Click the **Edit** icon to edit the Script Name and the description.
4. Click the **Download** icon to download the script to the local machine.

Adding a Script

To add a script:

1. Click **Add** and enter the information below.

   Script Name: Enter a name for the script
   Description: Enter a description for the script.
   Upload: Click browse to select a script from the local machine to upload to the STM server.

Editing a Script

To edit a script:

1. Click Edit and enter the information below.

   Script Name: Edit the name for the selected script
   Description: Edit the description for the selected script.
   Upload: Displays the script corresponding to the selection.

Policies

The STM server has the capability of configuring multiple agents at once using policies. Polices are for advanced users. Typically the default policies will not need to be changed.

IMPORTANT: An agent can belong to only one policy. If you move an agent from one policy to another, all settings (even ones set specifically for that agent) are overwritten to the values of the policy.

Policies allow you to configure sets of agents to behave similarly and to push configurations out to the agents. The server builds a list of configuration parameters to push for each agent then proceeds to push the parameters to each agent. When you push a policy out to its agents, all parameters are pushed. The agent compares the incoming parameters to current ones and updates the policy. After updating the agent is restarted.

For example: If an agent is performing file analysis, and you push a new parameter (ex: new file analysis rule), the configuration will be updated and the module restarted (file analysis is terminated). File analysis will start at the next regularly scheduled start.

Protection: You can protect an agent from being updated by the policy setup push to preserve special setups on a specific agent.

For example: On a critical server you may want the performance interval to be 1 minute, but on other servers you want the interval to be 5 minutes. To accomplish this configuration, you would define the policy setup performance frequency at 5 minutes and then use the monkey wrench to configure the critical server to 1 minute. The configuration for the one agent is automatically "protected" and will be unaffected by changes to the policy. This setting will only be overwritten in two cases:

- When you configure a policy, you check the **"override protection"** box.
- If you move the agent from one policy to another.

Override Protection: You can also override protection when you need to. When choosing the agents to push parameter(s) to you can choose to override any protection on the agent.

Note: This override is for all parameters you select on a push, not parameter by parameter (unless you push them one at a time). So for the above example, if you want to change a parameter (for example: Disk Usage threshold) on the protected agent, you could do so by selecting **Yes** for the Override Protection on the Push screen.

Self-Configure: When a new agent registers it automatically adds itself to the configuration push list (for all parameters). This function allows you to quickly set up all your agents during installation. As soon as the STM Server is running you should configure Policy Setup parameters so any agents that self-register subsequently will have the configuration you want.

Monitoring: You can also monitor the push list to see the progress of your configuration. From the push report, you can see pending pushes, as well as failures.

Notification of Failures: If the server cannot push a configuration to a server, it will try once an hour for twenty-four hours, and then abort the push. When it aborts, it also sends a trap to the Event Receiver, which can then notify you of the failure.

Policy List Page

The Policy List page allows you to add, edit, delete, or push all configuration parameters out to devices configured in the policy.

To create a new policy:

1. Click **New Policy** and follow the onscreen instructions.

To export policies:

1. Click **Export.**

The rules and policies will be saved as a SQL file. A simple execute this SQL file against the database is done to import the settings back when needed.

To edit the policy:

1. Click the **Edit** icon.

Once the policy has been edited you will need to push the policy out.

To push the policy to the configured devices:

1. Click on the **Policy icon.**

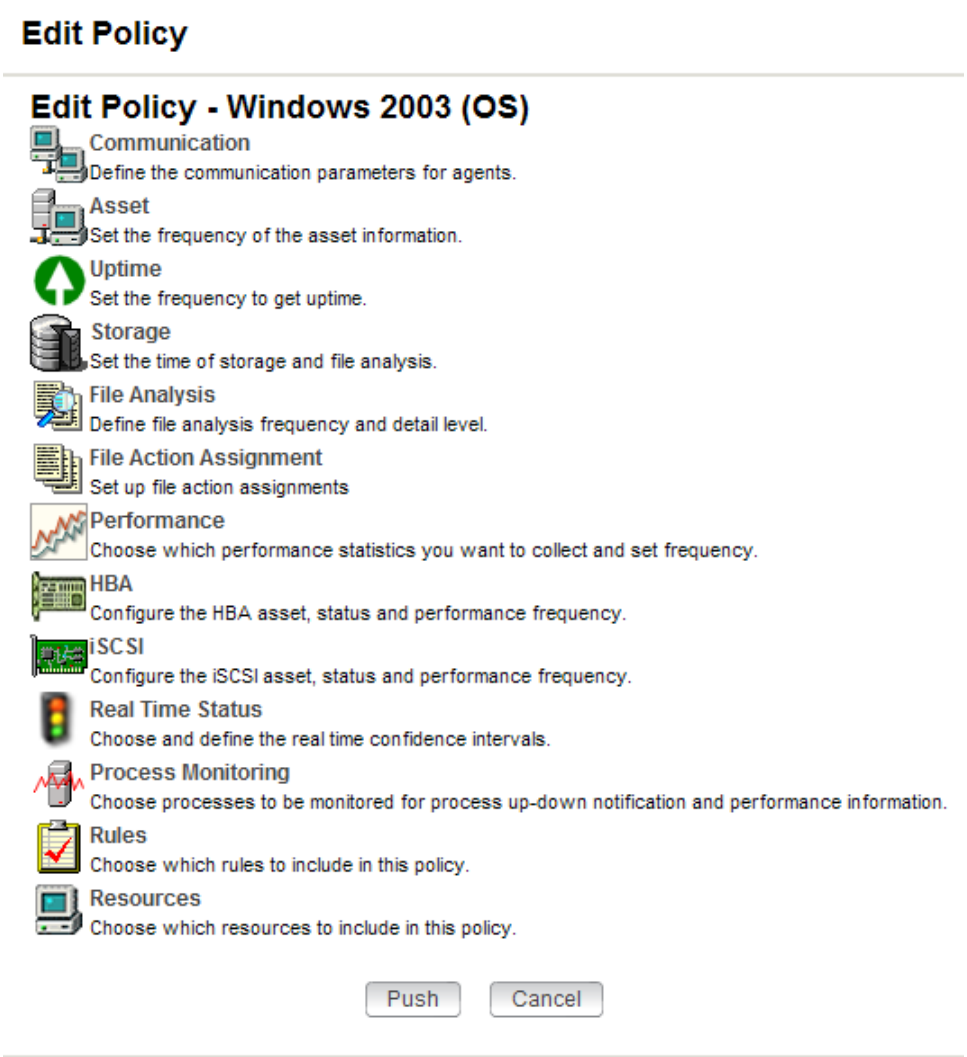
You can get a push list report by selecting **Push List Report.**

Creating a Policy

To create a new policy:

1. Click **New Policy.**
2. Enter the necessary information
    - **Policy Class:** The type of policy that you are creating (OS, Magnitude, etc.)
    - **Base Policy on:** Use a predefined policy as a template for the design of the new policy.
    - **Name:** The name that is assigned to the policy.
3. Click **Save.**

4. Define any necessary configurations and then click **Push.**
5. The **Push List Report** link displays a list of pushed agents/modules/policies.


Edit Policy
Edit Policy - Windows 2003 (OS)
Communication
Define the communication parameters for agents.
Asset
Set the frequency of the asset information.
Uptime
Set the frequency to get uptime.
Storage
Set the time of storage and file analysis.
File Analysis
Define file analysis frequency and detail level.
File Action Assignment
Set up file action assignments
Performance
Choose which performance statistics you want to collect and set frequency.
HBA
Configure the HBA asset, status and performance frequency.
iSCSI
Configure the iSCSI asset, status and performance frequency.
Real Time Status
Choose and define the real time confidence intervals.
Process Monitoring
Choose processes to be monitored for process up-down notification and performance information.
Rules
Choose which rules to include in this policy.
Resources
Choose which resources to include in this policy.
Push
Cancel

Editing a Policy

To edit the Policy Setup menu:

1. Click on the **Settings** link in the left navigation tree.
2. Under **Device Management** select **Policies.**

The Menu will show different sections of parameters that you can edit.

3. To edit a section click on the icon.

Once you have completed setting all the parameters you can push one or more parameters to one or more agents via the Push screen.

Interacting with the thwack User Community

thwack.com is a community site developed to provide users and the broader networking community with useful information, tools and valuable devices related to SolarWinds network management solutions

Providing Feedback

thwack also offers the ability to submit product feedback and feature requests via the STM Feature Requests forum. You may navigate to that forum via the thwack forums page.

Chapter 10

Linux Installation

The following sections detail the installation steps for LINUX.

Note: 32bit agent/server should only be installed on 32bit linux system
64bit agent/server should only be installed on 64bit linux system

STM Installation for LINUX

Supported Platforms - STM Server

Operating System	Supported Versions
Linux (Intel-32)	RedHat, SUSE
Linux (x86-64)	RedHat, SUSE

Supported Platforms - STM Agent

Operating System	Supported Versions
AIX (PPC 64)	5.0+
HP-UX (PA-RISC)	11
HP-UX (Itanium-64)	11
Linuxx86l-32)	Redhat, SUSE
Linux(x86-64)	Redhat, SUSE
Solaris (Sparc 32/64 bit)	8,9,10
Solaris (x86-32)	10

The agent install does NOT require a reboot.

Note: In case of RHEL 5/OEL 5 install, certain libXP packages are not installed along with the default RPM Packages. These are needed for STM to work correctly on Linux. Hence they have to be installed manually. Packages details: libXp-1.0.0-8.1.e15 and libXp-devel-1.0.0-8.1.e15 (These packages are available on the RH5 distribution DVD)

New Install for Linux Server

The following provides steps for installing STM on a new Linux Server.

Note: 32bit agent/server should only be installed on 32bit linux system
64bit agent/server should only be installed on 64bit linux system

To install on a Linux server:

1. Login as root.
2. Execute the install binary: `# ./Storage_Manager_Agent-linux-x86_32.bin`
3. Installation may take several minutes. You will be prompted for the following: -

Destination Path: The path where you want to install the agent. A directory will be created underneath this path if it does not already exist.

Agent Port: Correlates to the web services port that is used by the server to communicate with the agent. The default port '4319' is recommended.

Server Trap Port: Also related to the agent setup, the 'Server Trap Port' must be set to the port listening on the server for incoming trap events. The default port '162' is recommended.

Database Password: The password needed to access the database. It is important to write it down and keep it in a safe place. This password is used by the STM services to access the database, it is NOT the password used to login to the GUI.

4. To start the server, execute the following:
   `#/usr/bin/storage_manager_server start`

Note: To stop the server:

```
#/usr/bin/storage_manager_server stop
```

New Install for Linux Agent

The following provides steps for installing STM agents on a Linux Server.

Note: 32bit agent/server should only be installed on 32bit linux system
64bit agent/server should only be installed on 64bit linux system

To install on a Linux agent:

1. Login as root.
2. Execute the install binary:

```
# ./Storage_Manager_Agent-linux-x86_32.bin
```

3. Installation may take several minutes. You will be prompted for the following:

Destination Path: The path where you want to install the agent. A directory will be created underneath this path if it does not already exist.

Server IP Address: The IP address of the device running the STM server

Agent port: The agent server port to use.

4. To start the agent, execute the following:

```
#/usr/bin/storage_manager_agent start
```

Note: To stop the agent: `#/usr/bin/storage_manager_agent stop`

Uninstalling the Linux Server

The following section details how to uninstall a Linux server.

To uninstall a Linux agent:

1. Login as root.
2. Go to install path: # cd /opt/Storage_Manager_Server
3. Execute the Uninstall folder: # ./uninstall -mode silent
4. This will uninstall the STM Server.

Uninstalling the Linux Agent

The following section details how to uninstall a Linux agent.

To uninstall a Linux Agent:

1. Login as root.
2. Go to install path: `# cd /opt/ Storage_Manager_Agent`
3. Execute the Uninstall folder: `# ./uninstall -mode silent`
4. This will uninstall the STM Agent.

Upgrading a Linux Server on an Existing Installation

The following section details how to upgrade an existing Linux server.

To upgrade a Linux server:

1. Login as root.
2. Execute the install binary:

```
# ./Storage_Manager_Server-linux-x86_32.bin
```

3. Installation may take several minutes. You will be prompted for the following:

Destination Path: The path where you want to install the agent. A directory will be created underneath this path if it does not already exist.

Agent Port: Correlates to the web services port that is used by the server to communicate with the agent. The default port '4319' is recommended.

Server Trap Port: Also related to the agent setup, the 'Server Trap Port' must be set to the port listening on the server for incoming trap events. The default port '162' is recommended.

Database Password: The password needed to access the database. It is important to write it down and keep it in a safe place. This password is used by the STM services to access the database, it is NOT the password used to login to the GUI.

4. To start the server, execute the following:

```
#/usr/bin/storage_manager_server start
```

Note: To stop the server:

```
#/usr/bin/storage_manager_server stop
```

Upgrading the Linux Agent on an Existing Installation

The following section details how to upgrade an agent on an existing Linux server.

To upgrade an agent:

1. Login as root.

2. Execute the install binary:

```
# ./Storage_Manager_Agent-linux-x86_32.bin
```

3. Installation may take several minutes. You will be prompted for the following:

Destination Path: The path where you want to install the agent. A directory will be created underneath this path if it does not already exist.

Server IP Address: The IP address of the device running the STM server

Agent port: The agent server port to use.

4. To start the agent, execute the following:

```
#/usr/bin/storage_manager_agent start
```

Note: To stop the agent: `#/usr/bin/storage_manager_agent stop`

Backup Profiler Requirements

- CA ARCserve
- CommVault
- EMC/Legato NetWorker
- IBM TSM
- Symantec Backup Exec
- Symantec Veritas NetBackup

CA ARCserve:	
Versions/Models	10,11,12 (Windows), ARCserve 11.x (Linux)
Features	Activity
Supported Platforms	Windows (thru 12.x) and Linux (thru 11.x)
Requires Agent?	Yes – on ARCserve server
Requires a Proxy Agent?	N/A
Prerequisites	Location of ARCserve Install
Credentials	Windows – Local System account/Domain Account UNIX – run as root user
Read/Write Actions	Read Only
Ports Used	Profiler Data Collector/Agent Ports
Communication	See the See the STM Ports section below

CommVault	
Versions/Models	7.x, 8.x
Features	Activity Configuration Media Exceptions/Errors

Supported Platforms	Windows
Requires Agent?	No – to collect Activity, Configuration, Media Yes – on CommServ to collect exceptions/errors
Requires a Proxy Agent?	Yes – via STM servertrfg xsd if not collecting exceptions/errors
Prerequisites	Windows/ AD account to access CommServ (MS-SQL) database
Credentials	Windows - Local System account/Domain Account
Read/Write Actions	Read Only
Ports Used	STM Data Collector/Agent Ports
Communication	See the STM Ports section below
EMC/Legato NetWorker	
Versions/Models	6.x thru 7.4.4
Features	Activity Configuration Media Exceptions/Errors
Supported Platforms	Windows, Solaris, Linux, HP-UX, AIX, Tru64
Requires Agent?	Yes – on NetWorker Server
Requires a Proxy Agent?	N/A
Prerequisites	• If Regional settings for date/time is not United States, a Domain Account with regional settings of United States to be defined (Windows) • Location of Networker install • Date format of Daemon.raw (NetWorker 7.4)
Credentials	Windows - Local System account/Domain Account UNIX – Run as root user
Read/Write Actions	Read Only
Ports Used	STM Data Collector/Agent Ports
Communication	See the STM Ports section below
IBM TSM	
Versions/Models	5.x
Features	Activity Configuration Storage Pool Media Exceptions/Errors
Supported Platforms	Windows, AIX, Linux
Requires Agent?	Yes – on Master Server or on server with DSMADMC
Requires a Proxy	N/A

Agent?	
Prerequisites	• Account to access TSM database with operator privileges • Location of TSM BA client install (on proxy agent/master server) • TSM BA client options file (dsm.opt) configured for access to 1 or master servers • TSM Instance name
Credentials	Windows - Local System account/Domain Account UNIX – Run as root user
Read/Write Actions	Read Only
Ports Used	• STM Data Collector/Agent Ports • TSM BA client communicates on port 1500(configurable) of the TSM Master Server
Communication	See the STM Ports section below
Symantec Backup Exec	
Versions/Models	8.x, 9.x, 10.x, 11.x, 12.x
Features	Activity
Supported Platforms	Windows, NetWare
Requires Agent?	Yes – on Master server
Requires a Proxy Agent?	N/A
Prerequisites	• Location of Backup Exec install • Login to MS-SQL Server database • Date Format of Set and Job (found in Backup Exec logs)
Credentials	• UNIX - Run as root • Windows - Local System account/Domain Account • Netware - Local admin • * Account and password stored in Profiler database and configuration files on proxy agent using custom encryption
Read/Write Actions	Read Only
Ports Used	STM Data Collector/Agent Ports
Communication	See the STM Ports section below
Symantec Veritas NetBackup	
Versions/Models	4.5.x, 5.x.x thru 6.5.3.1
Features	Activity Configuration Media Exceptions/Errors Tape Drive Utilization

Supported Platforms	Windows, Solaris, Linux, HP-UX, AIX
Requires Agent?	Yes – on Master Server
Requires a Proxy Agent?	N/A
Prerequisites	Location of NetBackup Install
Credentials	UNIX - Run as root Windows - Local System account/Domain Account
Read/Write Actions	Read Only
Ports Used	STM Data Collector/Agent Ports
Communication	See the STM Ports section below

Installing Agents on Windows Cluster (Windows 2008)

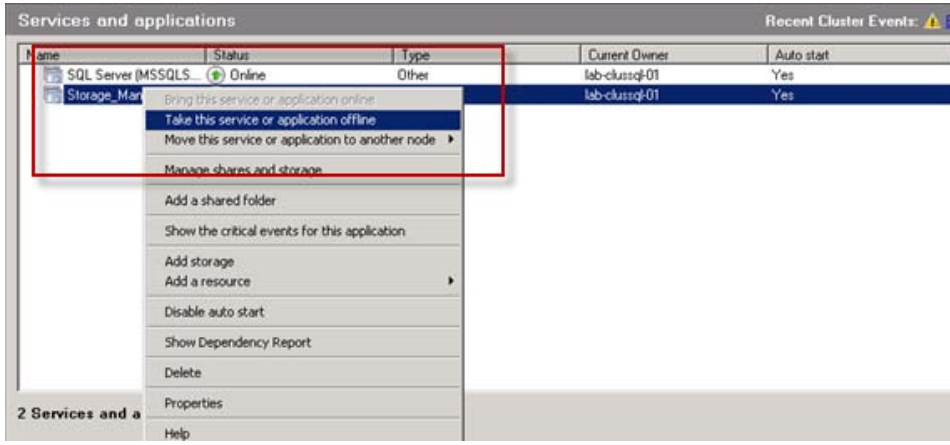
The following steps detail the installation of STM agents onto a Windows Cluster.

1. Login remotely to the Active node of the cluster as **Local Administrator**.
2. Execute the installer.
3. Enter the destination path where you want to install the agent, select the location on the shared drive. Next, Enter the **Server IP Address** of the STM Server.
4. Leave remaining options set to default.
5. **Do Not Start** the Agent. Click **No** when prompted.
6. After the agent is installed on this node in the cluster, failover to the other node and follow the steps above.

Note: When prompted, select the same destination path previously selected.

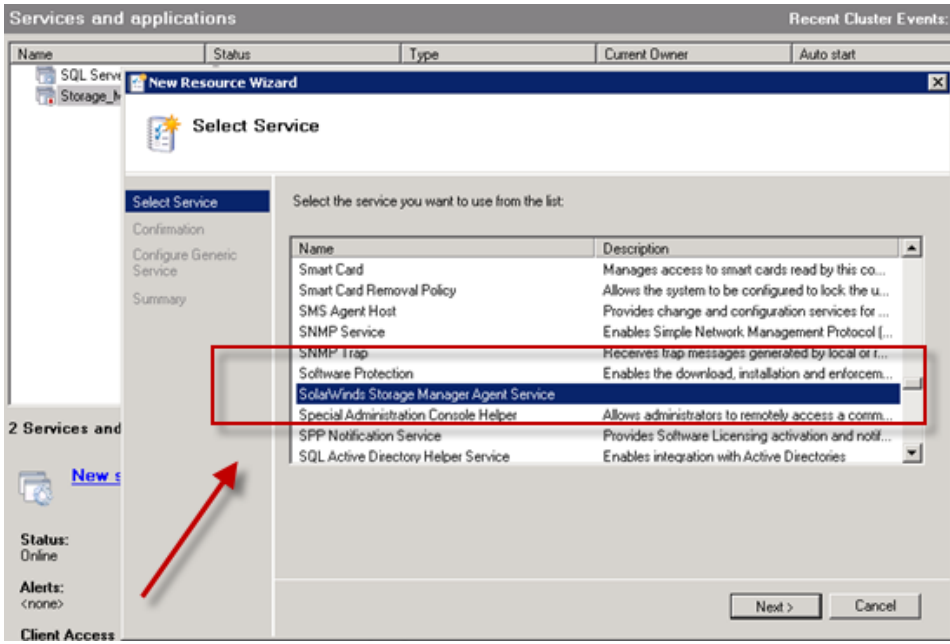
To create a new cluster device:

1. Remotely login to the server with the virtual IP Address.
2. Click **Start > All Programs > Administrative Tools > Failover Cluster Manager**.
3. Right click on **Services and Applications > More Actions > Create Empty Service or Application**.
4. Right click **Create Empty Service or Application > Properties >** give a proper name and save it.
5. Next Right click on the service and **Take this service or Application Offline**.



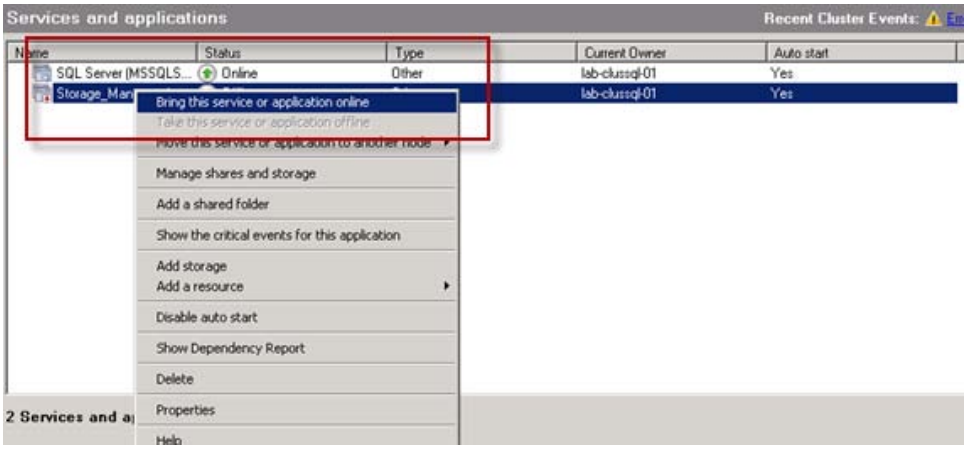
6. Right click the offline Server and select **Add a Device > Generic Service.**

7. Select **SolarWinds Storage Manger Agent Service** from the list and click **Next.**

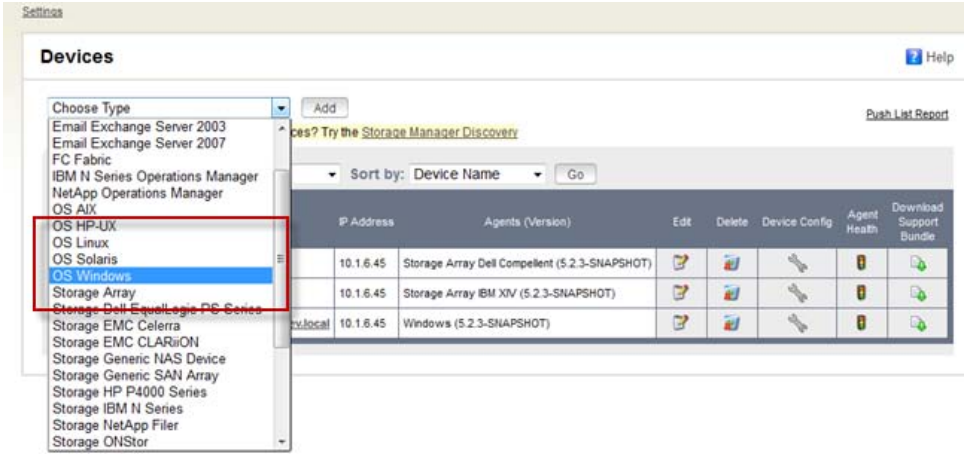


8. Click **Finish**.

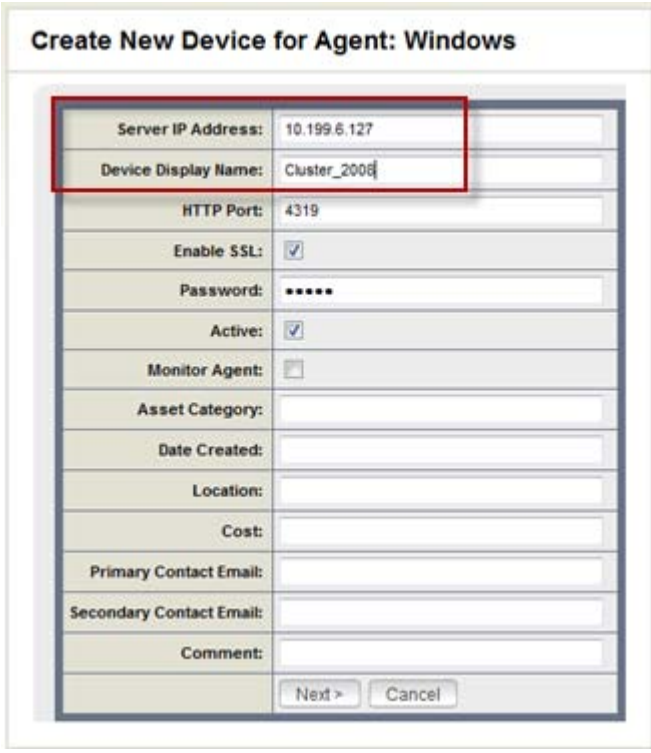
9. Right click and select **Bring the service or application online**.



10. Next you will need to login into **Storage Manager** web console, then click **Settings > Device Management> All Devices > Choose Type> OS Windows > Add**.



11. Enter the **Virtual IP Address** of the cluster and provide a **Display Name**.



12. Click **Next** and **Save**.

Appendix

SMI-S Provider Installation & Configuration

This section covers the installation and configuration of SMI-S Providers for your arrays.

Each section is followed by troubleshooting steps and FAQs for each SMI-S Provider.

Select your array from the table below:

3PAR	EMC Vmax	HP Lefthand	Pillar
Dell MD3K	HDS (Hitachi)	IBM DS	Sun Storage TEK 99XX
Dell Compellent	HP	IBM SVC	Sun Storage TEK 2k, 6K & FLX
EMC Clariion	HP XP	LSI	EMC Text Provider Tool
EMC Symmetrix	HP EVA	Solaris	SMI-S Test Provider Tools

General SMI-S Questions

Q: What is SNIA and SMI-S?

A: SNIA is the Storage Networking Industry Association in-charge of SMI-S. SMI-S is the Storage Management Initiative – Specification. SMI-S uses CIM (Common Information Model) to model a storage device.

SNIA official website: http://www.snia.org

Q: What Storage Array venders support SMI-S?

A: EMC, LSI, HP, IBM, 3PAR, Pillar, HDS, Fujitsu

Q: What is a provider?

A: A provider is a CIMServer which handles CIM requests from a CIMClient. Using the vender's API, the provider connects to the device and translates it into CIM. This enables CIMClients to make generic requests across a heterogeneous environment.

Q: Which Storage Arrays have embedded providers?

A: 3PAR, Pillar, Symmetrix V-Max Series

Q: What are the Default Ports used by the providers?

A: The default ports are 5988 for http traffic and 5989 for https traffic.

Note: Before installing the Provider, run netstat to make sure the default ports are not being used. If another Cimom or IBM Director (http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp?topic=/diricinfo/fqm0_r_tbs_cimserver_openwbem_port_conflict.html) is running on the machine, changing the port the Provider listens on will be required for the Provider to run.

Default Namespaces

Vendor	Namespace
LSI	root/lsissi11
3PAR	root/tpd
EMC	root/emc
HP	root/eva
IBM	root/ibm
HDS (versions after 5.8)	root/smis/current
HDS (versions prior to 5.8)	use /root/hitachi/dm<xx> where xx is version

SMI-S Providers

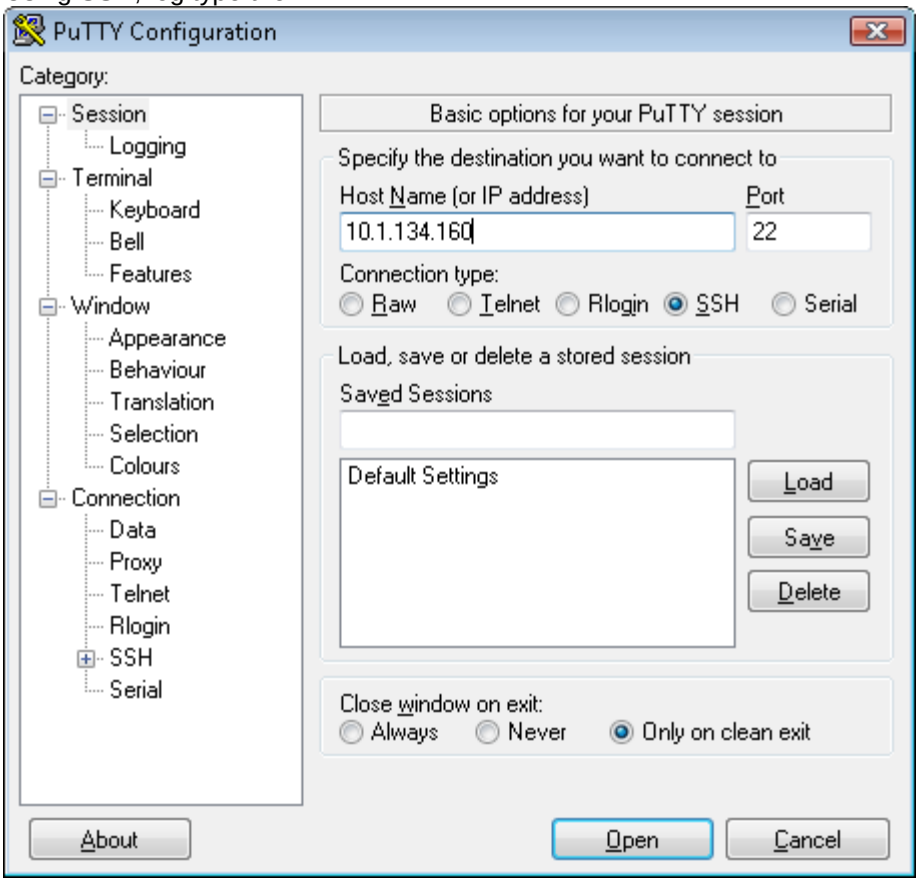
The following sections detail various vendors SMI-S Provider installation steps and troubleshooting FAQs.

3PAR Provider

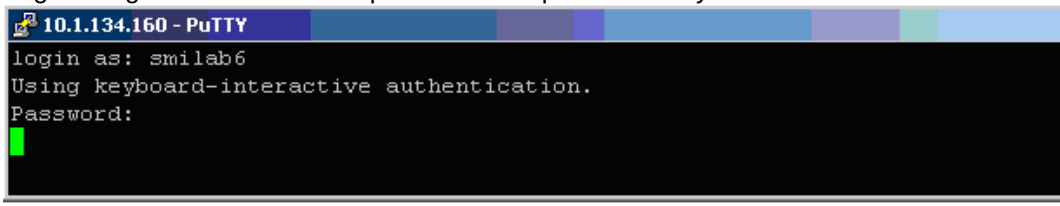
The 3PAR provider is embedded into the Storage Array, no need to install a Provider.

Logging into the CLI

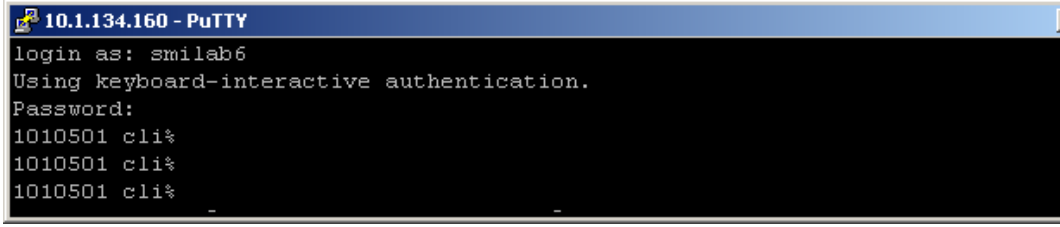
Using SSH, log type the IP



Login using the username and password setup on the Array.



You should see the following after successfully logging in.



Note: By default the Provider is disabled and must be enabled by an administrator.

Troubleshooting 3PAR

The following section list frequently asked questions for the provider.

Q: What is the default username and password?
A: 3paradm / 3pardata

Q: How do I enable the Provider?
A: Logon to provider as described above and call “setcim” command
This command can be used to enable or disable certain services on the Provider.

Q: How do I know if the Provider is running?

A: InForm OS version 2.2.3, logon to provider as described above and call type “showcim”.

Note: In previous versions, from a remote machine, telnet to the Array on port 5988.
Example: telnet 10.1.134.160 5988.

Q: How do I get the version of InForm OS?

A: Logon to provider as described above and call “show version”.

Q: How do I get an explanation on the commands I am running?

A: Logon to provider as described above and call “help”. For help on a particular command, type “help <command>” where <command> is the command for help needed.
Example: “help show”.

Q: How do I start the Provider?

A: Logon to provider as described above and call “startcim” .

Q: How do I stop the Provider?

A: Logon to provider as described above and call “stopcim”.

Q: How do I exit the CLI?

A: Logon to provider as described above and call “quit”.

Q: What is the minimum InformOS firmware supported version for the 3PAR array?

A: 2.3.1.

Dell MD3K Provider

The Dell MD3K series can be monitored from any OS agent by polling an LSI SMI-S Provider.

Dell Compellent

For version 5.5.4 only. You will first need to create a local user on the server where Compellent Data Collector Manager is installed.

1. Login to the Windows server where the Compellent Data Collector Manager is

installed.

2. Create a Windows Local User account with 8 characters or less - DO NOT USE Special

Characters.

   a. User Example: cmuser
   b. Use any Alphanumeric password
   c. Password Example: storage123

3. Add the Windows local user account to the Administrators Group
4. Give the User Account rights to logon as a Service.

a. **All Programs > Administrative Tools > Local Policies > User Rights Management**.

b. Double click on Log on as a service Policy.

5. Add the user and then apply the changes.

6. Important: Log off and Login to the server with the new Windows Local User account you've just created.

Example User: cmuser

7. Create a New User for Compellent Enterprise Manager

Note: If open security is used, the user can be added from the Enterprise Manager Client.

a. Login to Compellent Enterprise Manager.

b. Type the username you used for the Local Windows Account that was created.

c. User Example: cmuser

d. Click the Check box Create New User.

e. Type an alphanumeric password with LESS than 8 characters and **NO Special Characters.**

f. Password Example: STM1234.

g. Click **Login**.

8. Once the New User has been created click the Add Storage Center button to add it to the

user or click the Management menu item at the top left of the screen.

a. Use the Admin credentials to add the Storage center to the user.

Note: If an Advanced security policy is used, add the user from the Data Collector Manager

Interface.

9. Open the Compellent Data Collector Manager GUI.

a. **Click > All Programs > Compellent Technologies > Compellent Enterprise**

Manager > Compellent Enterprise Data Collection Manager

b. Click **Properties**

c. From the User Viewer, confirm that the new user is now visible.

10. Set the Service Type and User in Data Collector Manager.

a. Click Service from the left pane.

b. Click Change at the bottom right in the Data Collector Service Properties. This

allows you to edit the configuration.

c. Click the Service User Type dropdown and change it to Local User Account.

d. Add the Service User Name and Password.

e. Use the Windows Local User Account and Password that was previoulsy created.

f. User Example: cmuser.

g. Password Example: storage123.

h. Click Apply Changes on the bottom right.

11. Configure SMI-S in Data Collector Manager.

a. Click SMI-S from the Left Pane – The SMI-S Server configuration will show in the

right pane.

b. Click Change at the bottom right in the SMI-S Server Configuration.

c. Select Enable SMI-S Server.

d. Uncheck Use Https for SMI-S server connections.

e. Check Manually Manage Users.

f. Click Apply Changes on the bottom right.

Add SMI-S User from CLI

12. Run the Command Prompt as Administrator.

a. Change directory to <Compellent install folder >\Compellent Enterprise Manager\msaservice\Pegasus\bin

b. Type: cimuser -a –u <username> -w <password>

c. User is the Compellent Enterprise Manager user created.

d. User Example: cmuser

e. Password is the Compellent Enterprise Manager password. The less than 8 character password used when creating the Enterprise Manager account.

f. Password Example: STM1234

g. Type: cimuser -l <enter> - This will verify the user has been added successfully.

h. Restart the Compellent Data Collector Manager service.

13. Adding the Compellent to SolarWinds Storage Manager software.

a. Login to SolarWinds Storage Manage.

b. Click Home on the upper left or go to Settings on the upper right and Click Getting

Started.

c. Click Add next to Storage Arrays.

d. Click the dropdown.

e. Select Dell Compellent.

f. Enter the Compellent Enterprise Manager username and password. This is the same

username and password created through the CLI (cimuser) command.

g. Example User: cmuser

h. Example Password: STM1234

i. Provider IP: <IP of the server running the Compellent Data Manager Collector>

j. Click Test.

k. Copy the bolded IP from the results screen.

l. Paste the copied IP into the Storage Center IP section.

m. Click Save.

Troubleshooting Compellent

What is the minimum version of Enterprise Manager supported?

Answer: v 5.5.4

Where can I find the version of Enterprise Manager running?

Answer: Open the Data Collector Manager GUI. If the service is running, there will be a shortcut in the system tray. **Right click > Show.** >Version will be displayed on the screen.

How to stop/start the SMI-S provider?

The SMI-S provider is NOT running as a separate service. It is running as a process under the Data Collector Manger Service. The service name is Compellent Enterprise Manager Data Collector. The process name of the smi-s provider is cimserver.

Q: Unable to connect or get data from the SMI-S Provider. How do I debug?

Answer: Step through the configuration steps and make sure everything is configured correctly

a. Check the Task Manager . Process list . Make sure the ‘cimserver’ is running.

b. Verify that the cimserver is listening on port 5988. (netstat -ano| find "5988")

Verify that SMI-S user is added correctly

a. From command prompt, run <Compellent install folder >\Compellent EnterpriseManager\msaservice\Pegasus\bin\cimuser -l

b. Open Data Collector Manager . Click Properties . Choose Log Viewer

c. Enable debug Logging

d. Open Data Collector Manager . Click Properties .Choose Debug Loggers

e. Check SMI-S, Compellent API, API XML Web Services

f. Apply the changes.

g. Debug Logs are located in <Compellent install folder>\Compellent EnterpriseManager\msaservice\etc\compservices\debuglogs

Note: Turn the debug logging off after collecting the logs.

Is there any info on the SMI-S provider available in the Data Collector Manager help?

Answer: Yes. Detailed instruction on setting up the SMI-S for the specific version installed is available in the help. Click HELP on Data Collector Manager startup screen. See the section under Using Dell Compellent SMI-S provider.

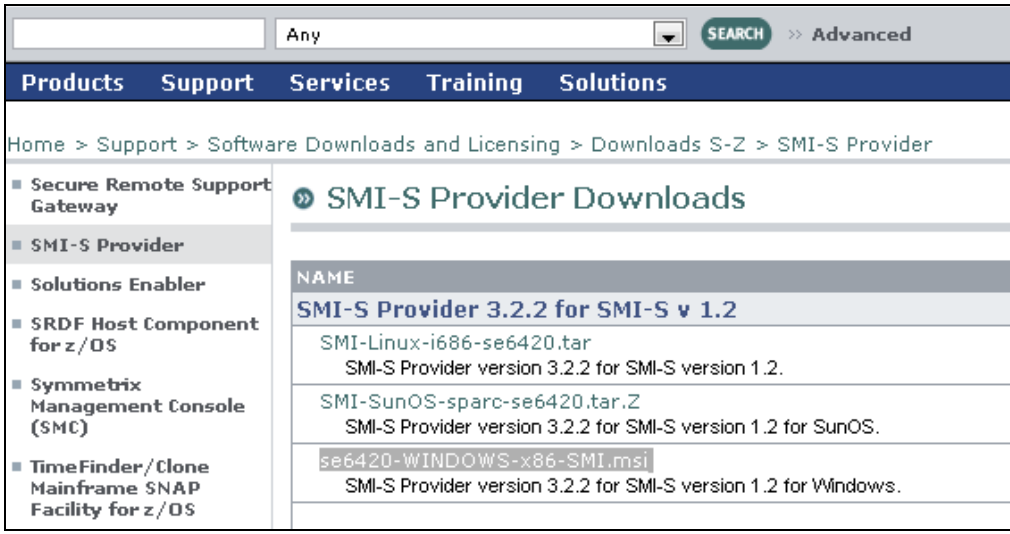
EMC Provider (Clariion, Symmetrix, Vmax)

The following section details installation steps for all versions of the EMC Provider.

Note: Do not install your EMC Provider where ECC is installed, if possible.

General Information:

Download: https://powerlink.emc.com
Location: Location: Home > Support > Software Downloads and Licensing > Downloads S > SMI-S Provider



Release Notes:
Home > Support > Technical Documentation and Advisories >
Software ~ S ~ Documentation > SMI-S Provider > Release Notes

Supported EMC Hardware and Firmware:

Supported Symmetrix arrays (supported with EMC Enginuity™ 5x67 or later)
Symmetrix DMX™ series (DMX-3, DMX-2, DMX-1)
Symmetrix 8000 Series
Supported CLARiiON arrays (supported with EMC Navisphere® Release 19, 22, 24, 26)
CX3 Series, CX Series, and AX Series

The support matrix document is available from

http://developer.emc.com/developer/devcenters/storage/snia/smi-s/downloads/EMC_Providers_SMI-S_Only.pdf

EMC Provider Version 4.0 and later

The following section detail installation steps for Windows and Linux.

Installation On Windows

1. Download the software from the Powerlink website.
2. Save all files and exit all Windows applications. Launch the self-extracting executable. For example: To install the EMC SMI-S Provider V4.0 software on a Windows platforms, launch the self-extracting executable, se7000-WINDOWS-x86-SMI.exe.
3. The EMC Solutions Enabler with SMI X86 welcome page appears prompting you to install Solutions Enabler with SMI version x.x. Click Next.
4. Click Next to begin the installation. The Destination Folder dialog box opens and prompts you to select an install directory for Solutions Enabler and EMC SMI-S Provider. It is recommended that you choose the default directory.
5. Click Next to continue. The Ready to Install the Program dialog box opens.
6. Click Install to begin installing files to your selected folder. This may take several minutes. The Installation Wizard Completed dialog box open.
7. Click Finish to complete the setup.

Service name is 'ECOM'.

Installation On Linux

1. Download the software from the Powerlink website.
2. Extract the TAR image to a temporary directory.
3. Change the directory to the location of the EMC SMI-S Provider kit and run the install script by using the following command:

cd /<location of extracted files or CD>/UNIX

se<xxxx>_install.sh -install

4. The installation program will begin copying the files. When complete, the installation program will automatically start the storapid daemon and the cimserver, which may take a few minutes.
5. When complete, the installation program will return the following confirmation message, which lists EMC Solutions Enabler with SMI-S Provider in the HAS BEEN INSTALLED list:

```
#-------------------------------------------------------------------
   -------------

# The following HAS BEEN INSTALLED in /opt/emc via the rpm
   utility.

#-------------------------------------------------------------------
   -------------

ITEM   PRODUCT                    VERSION
```

```
01     EMC Solutions Enabler     V7.0.0.0
SMI    KIT                       V4.0.0.0
#-------------------------------------------------------------------
    -------------
```

Logging In

6. Run the TestSmiProvider.exe (located at <install_dir>\ECIM\ECOM\bin).

7. Accept defaults for host, connection type and port.

Username : LocalDir/admin Password : #1Password

Symmetrix

Symmetrix arrays are discovered automatically by the provider. So it is not required to add it to the provider using 'addsys' command. The host where the provider is installed must have at least one LUN presented to it from the array. EMC recommends having at least 6 gatekeepers for getting better performance.

CLARiiON **Locally Attached**

A locally attached storage array is one in which at least one CLARiiON LUN is visible to the host on which the provider is running. The locally attached CLARiiONS are discovered automatically. But it requires the authorization information for each CLARiiON storage processor already added.

1. Confirm the array to be added is locally attached.

<install_dir>\SYMCLI\bin\syminq –cids

There should be at least one LUN mapped to this host from the array.

2. Check the OSLSProvider.conf setting has discover set to 'true'.

OSLSProvider.conf is located at <install_dir>\ECIM\ECOM\Providers folder.

OslProv/com.emc.se.osls.osl.StorApi.database.discover=true

3. List the authorization info.

<install_dir>\SYMCLI\bin\symcfg list auth

4. If the list does not have entries for SPA and SPB of this array,

stop the provider service(ECOM)

5. Add the authorization for SPA and SPB using,

<install_dir>\SYMCLI\bin\symcfg authorization add –host <host> – username <user> -password <pass>

where <host> is the IP Address of the storage processor.

6. Start the provider service.

CLARiiON out-of-band

Note: out-of-band CLARiiON are arrays which do not have any LUNs presented to the host where the provider is running.

1. Log into the Provider by following the steps from “Logging In”.

2. Run the addsys command.

3. Type “y” at Add System prompt.

4. Chose the Array Type 1 for Clariion

5. Type in the IP address of Storage Processor A and Storage Processor B

6. Type the Address type 2 for both Storage Processors

7. Type the Username and Password for a user with either Admin or Manager privileges on the Array.

Note: If the addition of the Array is successful, you will get an output of 0 when the Array is discovered.

The output should look like

```
++++ EMCAddSystem ++++

OUTPUT : 0

Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout, 4=Failed

       5=Invalid Parameter

       4096=Job Queued, 4097=Size Not Supported

System :
//172.28.5.35/root/emc:Clar_StorageSystem.CreationClassName="Clar
_StorageSystem",Name="CLARiiON+CK100060002000"
```

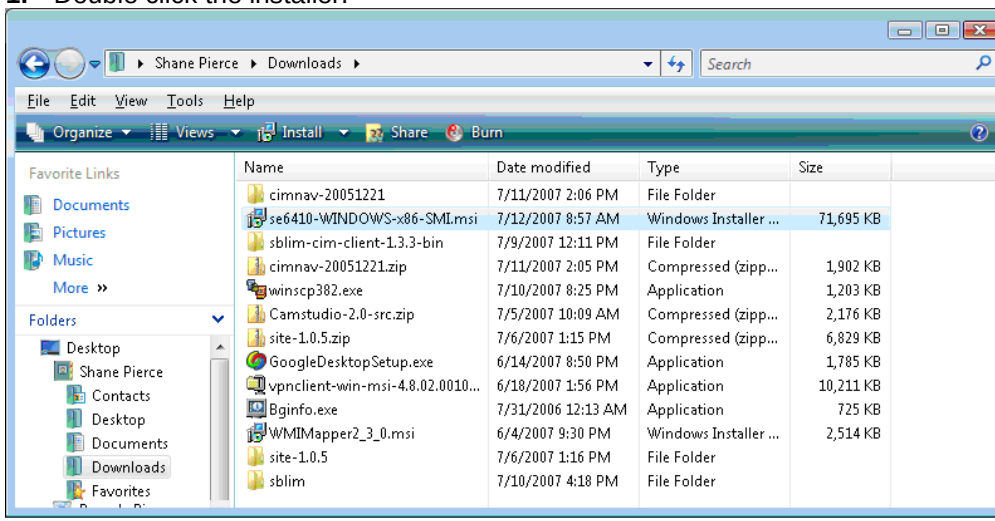
Make a Note of the Identifier (CLARiiON+CK100060002000 in the sample output shown above), which is required for configuring the Array in Profiler

Provider Version Pre-4.0.0

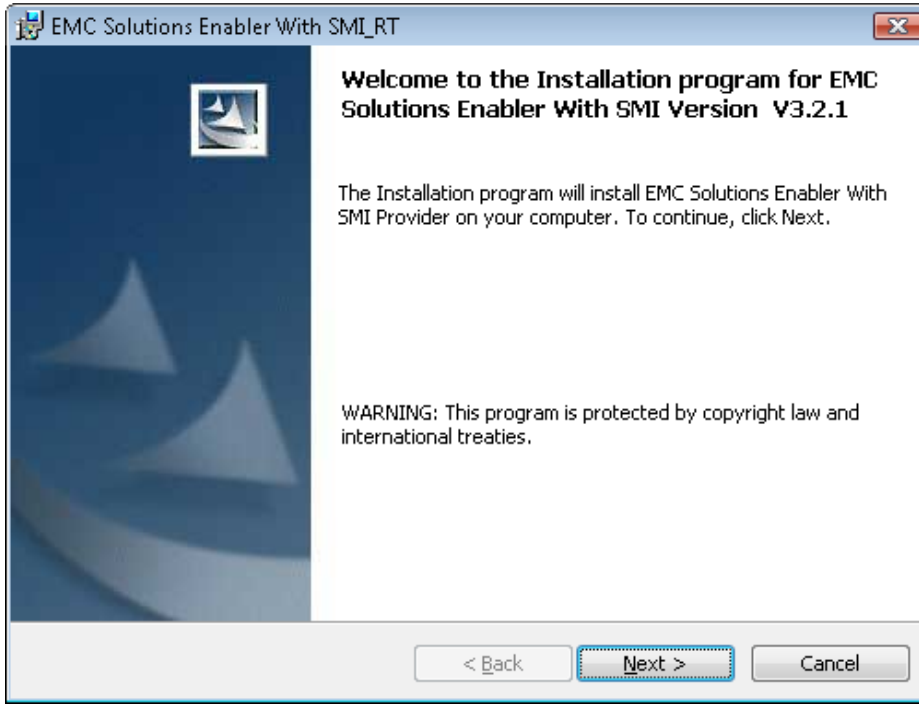
The following section detail installation steps for Windows and Linux.

Installation on Windows

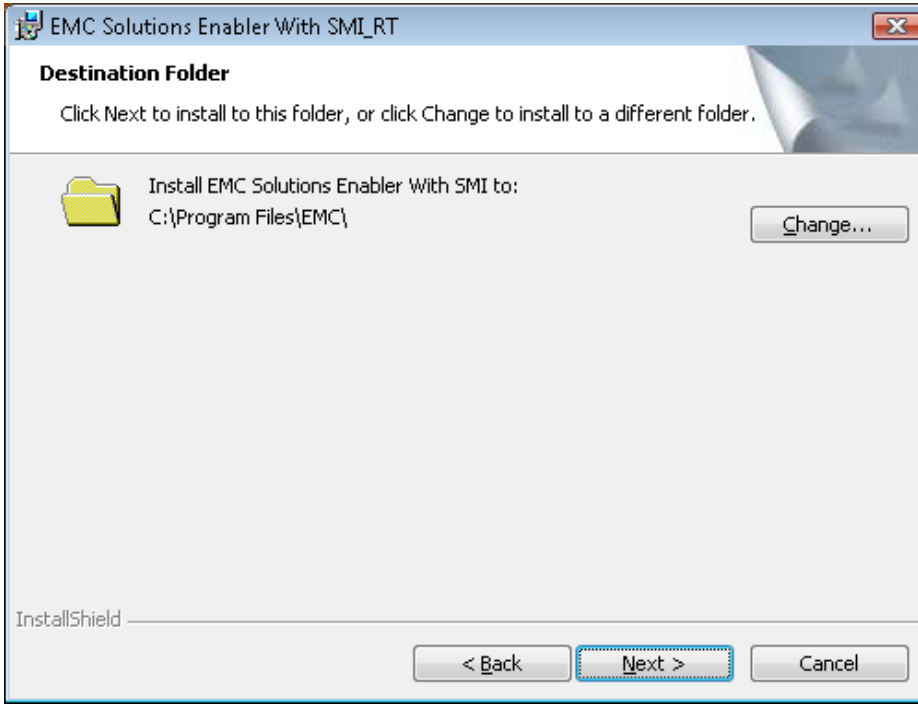
1. Double click the installer.



2. Click **Next** on the “Welcome” screen.

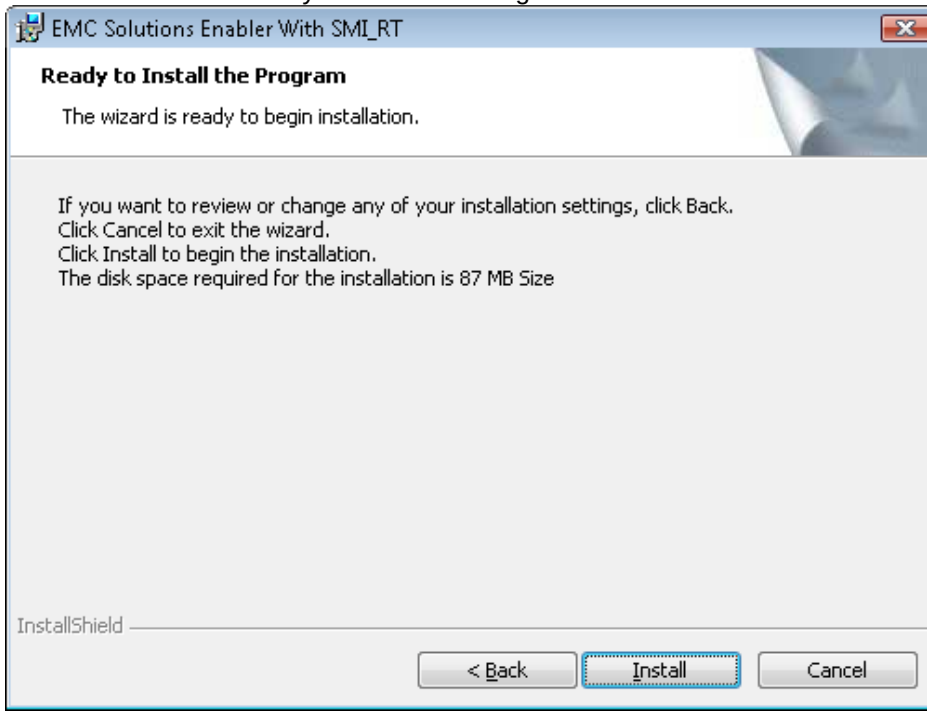

EMC Solutions Enabler With SMI_RT
Welcome to the Installation program for EMC Solutions Enabler With SMI Version V3.2.1
The Installation program will install EMC Solutions Enabler With SMI Provider on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

3. Choose a location to install to at the “Destination Folder” screen.

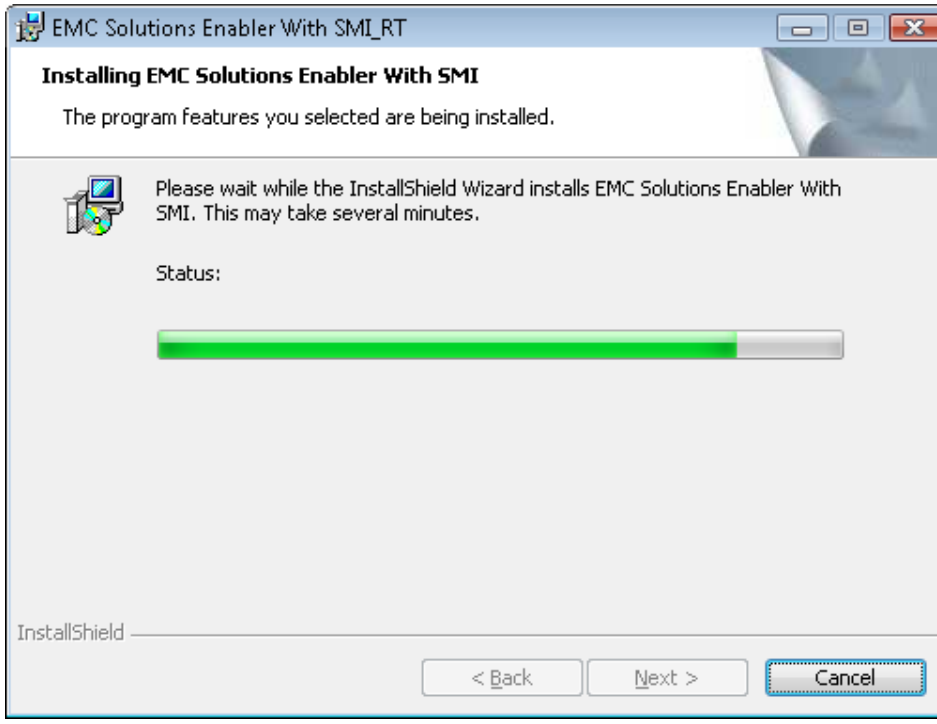

EMC Solutions Enabler With SMI_RT
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install EMC Solutions Enabler With SMI to:
C:\Program Files\EMC\
Change...
InstallShield
< Back
Next >
Cancel

4. Click **Next**

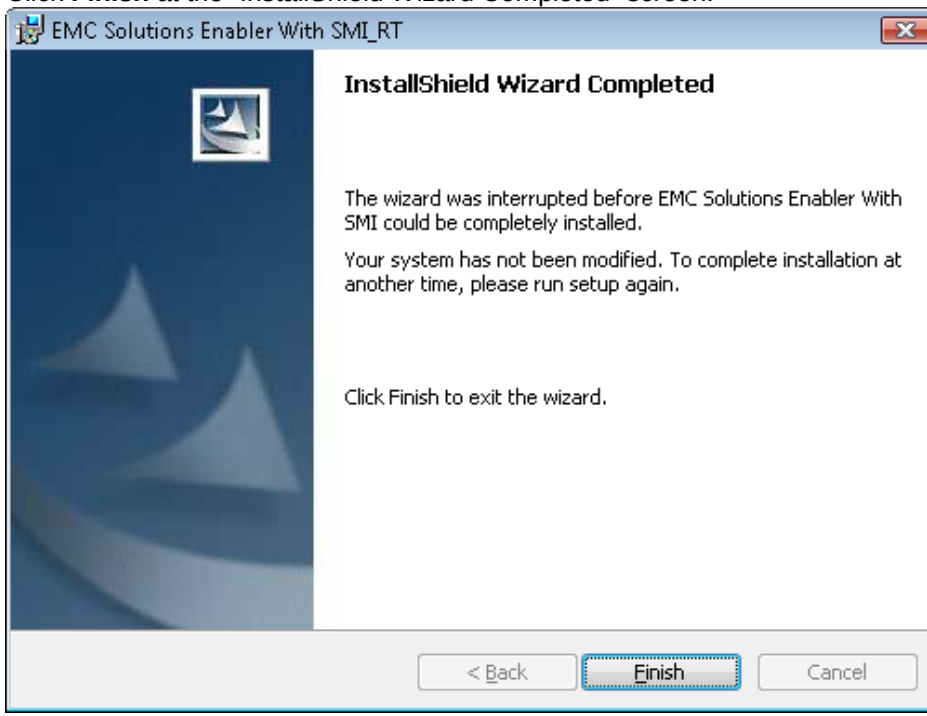
5. Click **Install** at the “Ready to Install the Program” screen.


EMC Solutions Enabler With SMI_RT
Ready to Install the Program
The wizard is ready to begin installation.
If you want to review or change any of your installation settings, click Back.
Click Cancel to exit the wizard.
Click Install to begin the installation.
The disk space required for the installation is 87 MB Size
InstallShield
< Back
Install
Cancel

6. You should see the “Installing EMC Solutions Enabler with SMI” screen:


EMC Solutions Enabler With SMI_RT
Installing EMC Solutions Enabler With SMI
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs EMC Solutions Enabler With SMI. This may take several minutes.
Status:
InstallShield
< Back
Next >
Cancel

7. Click **Finish** at the “InstallShield Wizard Completed” screen.


EMC Solutions Enabler With SMI_RT
InstallShield Wizard Completed
The wizard was interrupted before EMC Solutions Enabler With SMI could be completely installed.
Your system has not been modified. To complete installation at another time, please run setup again.
Click Finish to exit the wizard.
< Back
Finish
Cancel

Installation on Linux

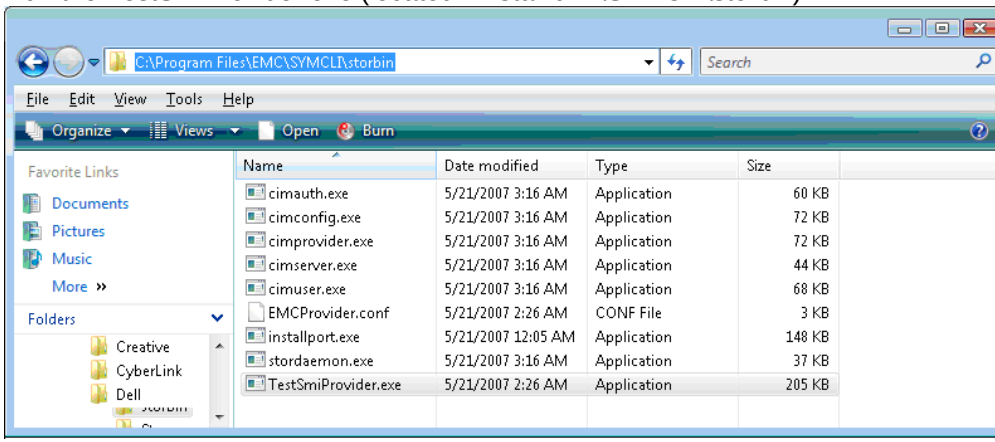
1. Untar the kit by typing: tar –xvf <filename>.tar
2. Execute the installer by typing: ./se6410_install.sh –install.

```
[root@red-box SMIKit]# ./se6410_install.sh -install

#------------------------------------------------------------------------
#                          EMC Installation Manager
#------------------------------------------------------------------------
Copyright 2007, EMC Corporation
All rights reserved.

The terms of your use of this software are governed by the
applicable contract.

Solutions Enabler Native Installer[SMI] Kit Location : /root/SMIKit

Checking for OS version compatibility......
Checking for previous installation of Solutions Enabler......
```

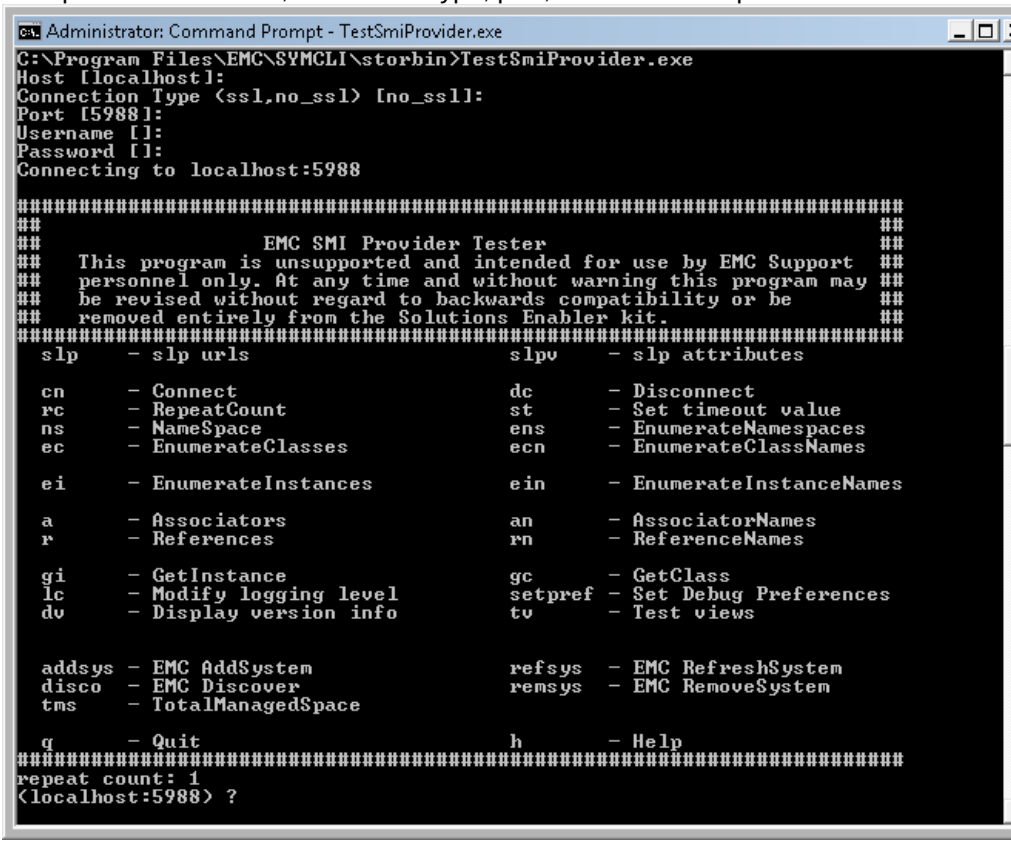
3. When the installer is finished, you will see the following:

```
Enabling stordaemon...

Starting storapid daemon..
 Waiting for daemon to start.  This may take several seconds.

Starting /usr/symcli/storbin/cimserver...


#-------------------------------------------------------------------------
# The following HAS BEEN INSTALLED in /opt/emc via the rpm utility.
#-------------------------------------------------------------------------
 ITEM  PRODUCT                                                  VERSION
 01    EMC Solutions Enabler                                    V6.4.1.0
 02    SMI  KIT                                                 V3.2.1
#-------------------------------------------------------------------------


[root@red-box SMIKit]#
```

4. Logging In
5. Run the TestSmiProvider.exe (located <install dir>\SYMCLI\storbin).



6. Accept defaults for host, connection type, port, username and password.


Administrator: Command Prompt - TestSmiProvider.exe
C:\Program Files\EMC\SYMCLI\storbin>TestSmiProvider.exe
Host [localhost]:
Connection Type (ssl,no_ssl) [no_ssl]:
Port [5988]:
Username []:
Password []:
Connecting to localhost:5988
EMC SMI Provider Tester
This program is unsupported and intended for use by EMC Support personnel only. At any time and without warning this program may be revised without regard to backwards compatibility or be removed entirely from the Solutions Enabler kit.
slp - slp urls
slpv - slp attributes
cn - Connect
dc - Disconnect
rc - RepeatCount
st - Set timeout value
ns - NameSpace
ens - EnumerateNamespaces
ec - EnumerateClasses
ecn - EnumerateClassNames
ei - EnumerateInstances
ein - EnumerateInstanceNames
a - Associators
an - AssociatorNames
r - References
rn - ReferenceNames
gi - GetInstance
gc - GetClass
lc - Modify logging level
setpref - Set Debug Preferences
dv - Display version info
tv - Test views
addsys - EMC AddSystem
refsys - EMC RefreshSystem
disco - EMC Discover
remsys - EMC RemoveSystem
tms - TotalManagedSpace
q - Quit
h - Help
repeat count: 1
(localhost:5988) ?

Adding A SAN

Symmetrix & CLARiiON Out-of-Band

Note: Out-of-Band CLARiiON are arrays which do not have any LUNs presented to the host where the provider is running.

1. Log into the Provider by following the steps from “Logging into the Provider”.

2. Run the addsys command.

3. Type “y” at Add System prompt.

4. Chose the Array Type to be monitored (1 for Clariion, 2 for Symmetrix).
Note: If choosing EMC Symmetrix, a LUN needs to be presented to the host where the EMC Provider is installed.

5. Type in the IP address of Storage Processor A and Storage Processor B if Clariion. Type the array id for Storage Processor A and Storage Processor B if Symmetrix
6. Type the Address type from step 5 above for both Storage Processors (2 if IP Address, 3 if Array ID).
7. Type the Username and Password for a user with admin or manager privileges on the Array.

repeat count: 1
(localhost:5988) ? addsys
Add System (y|n) [n]: y
ArrayType (1=Clar, 2=Symm) [1]:
One or more IP address or Hostname or Array ID
Elements for Addresses
IP address or hostname or array id 0 (blank to quit): 192.168.3.5
IP address or hostname or array id 1 (blank to quit): 192.168.3.6
IP address or hostname or array id 2 (blank to quit):
Address types corresponding to addresses specified above.
(1=URL, 2=IP/Nodename, 3=Array ID)
Address Type (0) [default=2]:
Address Type (1) [default=2]:
User [null]: admin
Password [null]: password

Note: If the addition of the Array is successful, you will get an output of 0 when the Array is discovered.

The output should look like

++++ EMCAddSystem ++++

OUTPUT : 0

Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout, 4=Failed

5=Invalid Parameter

4096=Job Queued, 4097=Size Not Supported

System :
//172.28.5.35/root/emc:Clar_StorageSystem.CreationClassName="Clar_Stor
a

geSystem",Name="CLARiiON+CK100060002000"

Make a Note of the Identifier (CLARiiON+CK100060002000 in the sample output shown above), which is required for configuring the Array in Profiler

CLARiiON Locally Attached

A locally attached storage array is one in which at least one CLARiiON LUN is visible to the host on which the provider is running. These arrays are automatically discovered and are not added using the addsys command.

8. Confirm the array to be added is locally attached.

<install_dir>\SYMCLI\bin\syminq –cids

There should be at least one LUN mapped to this host from the array.

9. Check the emcprovider.conf setting has 'discover'set to 'true'. It is located at <install_dir>\SYMCLI\storbin directory.

OslProv/com.emc.se.osls.osl.StorApi.database.discover=true

10. List the authorization info.

<install_dir>\SYMCLI\bin\symcfg list auth

11. If the list does not have entries for SPA and SPB of this array,

12. Stop the provider service.

13. Add the authorization for SPA and SPB using,

<install_dir>\SYMCLI\bin\symcfg authorization add –host <host> – username <user> -password <pass>

14. Restart the provider service.

Troubleshooting EMC (All Versions)

The following section details FAQs regarding troubleshooting issues.

Q: How do I find the version of the provider?

A: To find the provider version, do the following:

<install_dir>\SYMCLI\bin\symcfg –version

OR

Login to <install_dir>\SYMCLI\storbin\testsmiprovider

Execute the dv command.

Q: Why did I previously see Clariion performance in Profiler, and not now?

A: EMC's Provider pre-3.2.2 (SMI Kit pre-6.4.2) did not have any auto-synchronization with the array.

Q: Why is Profiler not recognizing changes in my array, and how do I resolve it?

A: The Provider does not recognize the change, when a LUN or RAID Group is created or deleted outside of the Provider (i.e. Navisphere). After that change is made, the refsys command needed to be run from testsmiprovider.

The 6.4.2 SMI Kit and higher has an auto-synchronization mechanism, which by default is one hour after the last update (this option is configurable). Upgrading the Provider to 6.4.2 or higher is a must when Profiler does not recognize changes in the array configuration.

Q: What EMC SMI Kit is needed for Flare Code 26?

A: EMC's SMIKit 6.4.2 (Provider 3.2.2) and higher. A Clariion with Flare Code 26 can only be monitored by an SMIKit 6.4.2 (Provider 3.2.2) or above. SolarWinds suggests installing EMC's latest version, patch 12.

Q: What port is used between the EMC Provider and Clariion?

A: Port 443 is used for bidirectional communication between the EMC Provider and Clariion.

Q: Why is Profiler not reporting on Clariion Performance?

A: Statistics logging must be turned on.

To enable Statistics Logging, do the following:

1. Open Navisphere.
2. Right click the icon for the storage system.
3. Click Properties.
4. Be sure SP A and SP B are in the System Level setting section.
5. Click the box for Statistics Logging under the Configuration section.

Q: What is the minimum flare code level that EMC recommends for the CLARiiONs to work with the EMC SMI Provider?

A: For release R26 → R26.031 for CX3 arrays and R26.028 for CX arrays

For release 28 → R28.707 for all arrays

For release 29 → R29.006 for all arrays

Q: What are some steps I can follow to get Clariion Performance in Profiler?

A: The following are some steps that can be followed:

1. Make sure Statistics are enabled for the array on SP A and SP B in Navisphere (Follow instructions in the section: Why is Profiler not reporting on Clariion Performance?).
2. For locally attached CLARiiONs, check if authorization info is present.(see section: Adding Authorization Info for Locally Attached CLARiiON.)

3. Run EMC TestSMIProvider and run the command ‘dv’. Make sure all array are discovered without any errors.
4. Make sure Performance frequency is set to non-off value in Wrench Icon for Storage Array in Profiler (i.e. Performance is turned on).
5. Make sure there are instances for class name CIM_BlockStorageStatisticalData when enumerating instance names (ein). To do this, do the following:
6. Run Tek-Tools testProvider or EMCs testSMIProvider (Logging In instructions above in Tools section).
7. Type ein for command.
8. Type CIM_BlockStorageStatisticalData for Class Name.

If no instances are returned, follow the instructions on resetting EMC provider (How do I reset EMC provider?). Once complete, repeat steps 1-3 again.

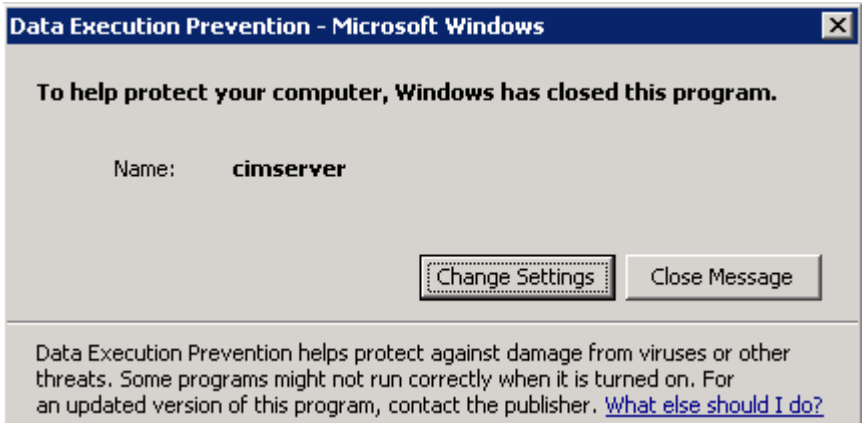
Q: I am getting WriteHitIOs always zero for the LUNs even though cache is enabled on CLARiiONs. Why?

A: This is due to a bug in the provider code. EMC will fix it in version 4.2.1 expected in July 2010. But the fix will only address CLARiiONs with flare code 30 or above.

Q: How do I get data for a CX600?

A: Per EMC, they do not support flare code 16 (2.16.x.x.x). The array must be upgraded to 19, 22, or 24 with all the latest patches for that release

Q: I get the following DEP error from windows for the SMI-s provider, how do I fix it?


Data Execution Prevention - Microsoft Windows
To help protect your computer, Windows has closed this program.
Name: cimserver
Change Settings
Close Message
Data Execution Prevention helps protect against damage from viruses or other threats. Some programs might not run correctly when it is turned on. For an updated version of this program, contact the publisher. What else should I do?

A: To enable DEP for the SMI-s provider, do the following:

1. Click Start. Click Run. Type sysdm.cpl, and then click OK.
2. On the Advanced tab, under Performance, click Settings.
3. On the Data Execution Prevention tab, use one of the following procedures:
4. Click Turn on DEP for essential Windows programs and services only to select the OptIn policy.
5. Click Turn on DEP for all programs and services except those I select to select the OptOut policy, and then click Add to add the programs that you do not want to use the DEP feature.
6. Click OK twice.
   The following link below gives a detailed description of hardware and software based DEP: http://support.microsoft.com/kb/875352

Q: What permissions are required when configuring a user in Navisphere?

A: You have to have an Admin or Manager privileges in order to discover.

NOTE: Monitor privileges are not enough.

Q: Why does the addsys command fail when trying to add an array to be monitored by the EMC Provider?

A: When running addsys, make sure of the following:

Make sure the user used has at least manager privileges.

Make sure that spA and spB are in correct order. To get the correct IP address for the storage processors, follow the instructions in the question "How do I get the IP address for the storage processors from Navisphere."

NOTE: Array ID 0 refers to spA, and Array ID 1 refers to spB.

Q: Why do commands like 'addsys' and 'dv' fails with "Error: CIM_ERR_FAILED: A general error occurred that is not covered by a more specific error code: provider initialization failed "?

A: Check whether the provider is installed on a 64-bit OS, if then check that provider installed supports 64 bit OS (Check in Provider Release Notes-→Supported Host Operating System). Provider installs including version 3.3 supports only 32 bit OS.

Q: How do I get the IP address for the storage processors from Navisphere?

A: To get the correct IP address from Navisphere, do the following:

1. Go to Navisphere
2. Right click on spA for the array you wish to add.

3. Click Properties.
4. Click Network. (This will show the IP address for spA).
5. Do steps 2 – 4 for spB.

Q: The server where we planning to install have a version of Solutions Enabler installed. How do I determine which version of the provider to use in this case?

A: Solutions Enabler is used by the provider as well as EMC management applications like ECC. It is better to install the provider on another server if possible. Otherwise, follow these steps to find out the correct version.

Check the version of the solutions enabler

<install_dir>\SYMCLI\bin\symcfg –version

The output show the version of the solutions enabler installed.

Check the solutions enabler version of the installer. It can be found from the name of the installer.

For Example: se65210-WINDOWS-x86-SMI.msi is packed with Solutions Enabler version 6.5.2.0

Install only if the versions match. If the version does not match, need to check and see if the solutions enabler can be upgraded to the required version without affecting ECC or other management applications already running there.

Q: Array Capacity (Raw) on the console screen shows non-zero value for Free capacity even though the Physical Disk Report shows that all disks are assigned to raid-groups. Isn't the free capacity representing the total capacity of the disks which are not assigned to any raid-groups?

A: This following response is from EMC.

The observed behavior is consistent with the way Clariion works. On Clariion, it is possible to see the primordial pool with RemainingManagedSpace having a non-zero value even though all disk drives are in use. In this situation, the value in the RemainingManagedSpace represents a collection of "left-over", unusable, disk capacities after the raid groups are created (i.e. concrete pools). For example, let's assume there are two disk drives available in a Clariion, with the capacities of 10 and 15 gigabytes. The client wishes to create a raid 1, raid group from these two disk drives. Because both disk drives should have the same size, the array uses the first disk drive with the capacity of 10 gigabytes and the first 10 gigabytes of the second disk drive. The remaining 5 gigabytes of the second disk drive will remain unused and is reported as a part of the RemainingManagedSpace capacity of the primordial pool.

One way to determine if all disk drives are in use is to examine the primordial pool's " EMCRemainingRawCapacity " property. If this property contains 0, it means all disk drives are in use by various concrete pools.

Q: EMC posted and End of Service Life for the Solutions Enabler and SMI-S provider, what are the versions affected and the end of life dates?

A:

Product	Version	EOSL Date
SMI-S Provider	3.0	10/2008
SMI-S Provider	3.1	10/2009
SMI-S Provider	3.2	10/2010
Solutions Enabler	5.5.1	9/30/2008
Solutions Enabler	5.4	9/30/2008
Solutions Enabler	5.5	9/30/2008

Q: Not getting storage data and ‘tms’ command shows error ‘invalid pool id’. Is this a known issue?

A: This happens when one or more pools use a really long name(longer than 32 chars). It is a known issue in provider versions upto 4.0.1.The work around is to change the pool name to a shorter one.

Q: Why is Symmetrix not showing correct number hosts masked into array?

A: Look at the symapi log file and look for following message:

‘SymDevMaskLoginHisto The VCMDB_RESTRICTED bit on symm 000187751584 is set, only records for this host will be returned’

This message means that the host the provider is running on needs to be able to obtain all the vcmdb info. EMC did not provide instructions on how to change this value and per EMC’s instructions ‘let the customer take care of it, he will know what to do or the storage administrator at that customer site will, it's not something you should attempt,you don't know the full story with regards to the san setup.’

Q: Can we use the EMC provider to monitor the CLARiiON behind the Celerra NS-20 device?

A: Yes, it works the same way as a regular Clariion

Troubleshooting EMC Version 4.0.0 and later

Q: LocalDir/admin no longer works in 4.1.1 provider, did the user name change?

A: Yes, username for 4.1.1 provider is now admin

Q: What files are needed to send a bug to EMC?
A: Any issues related to the EMC provider, EMC requires the following info before they’ll look into the problem:

All log files from <install_dir>\symapi\log

- All log files from <install_dir>\ECIM\ECOM\log
- symapi_db.bin file, located <install_dir>\symapi\db
- Output of the ‘dv’ command from the TestSmiProvider utility
- Output of the ‘tms’ command from the TestSmiProvider utility

Q: How do I change the port the provider listens on?

A: To change the port, do the following:

On the machine running the Provider:

1. Stop the ECOM Service
2. Navigate to <Install_dir>\ ECIM\ECOM\conf
3. Edit the properties of the file and uncheck “Read-only”, click ok
4. Open the file named port_settings.xml.

5. Change the port0 and port1 tag values to ports currently not in use.

For Example:<ECOMSetting Name="Port0">

<port>15988</port>

<secure>false</secure>

<slp>true</slp>

</ECOMSetting>

<ECOMSetting Name="Port1">

<port>15989</port>

<secure>true</secure>

<slp>true</slp>

</ECOMSetting>

6. Save port_settings.xml file.

7. Start the ECOM Service.

8. In the Profiler GUI: Go to Administration > Hosts.

9. Click the monkey wrench icon for the Array.

10. Change the HTTP port to the port set in the port_settings.xml on Provider.

11. Save the changes.

Q: How do I add a new user to the provider?

A: Login to the provider GUI.

1. Go to the URL https://<ipaddress>:5989/ecomconfig, and log in using the username LocalDir/admin and the password #1Password.

2. Click Add User and create a user with the role of Administrator. This newly created username can now be used to obtain access to the Array Provider.

Note: "LocalDir/' will prepended to the username whenever a new user is created.

For example: the new user name will be LocalDir/<the user name that you have given>

Q: How do I start/stop the provider from command prompt?

A: On Windows:

1. Stop → <install_dir>ECIM/ECOM/bin/sm_service stop ecom.exe

2. Start → <install_dir> ECIM/ECOM/bin/sm_service start ecom.exe

On Unix:

1. Stop → Obtain the PID of the ECOM process and issue the kill command for that PID. ie kill –SIGTERM [PID]

2. Restart → <install_dir>ECIM/ECOM/bin/ECOM –d

Q: How do I prevent locally attached Clariion from automatically being discovered?

A: Only provider version 4.0 and above. To remove a locally attached CLARiiON from auto discovery, write out a file with name 'claravoid' in the directory SYMAPI/config. The file must have the name of the CLARiiON.

Q: How do I prevent Symmetrix arrays from automatically being discovered?

A: Only provider version 4.0 and above. DO NOT use this method if the host where the provider is installed also has ECC running. Write out a file with name 'symavoid' in the directory SYMAPI/config. The file must have the SymmID of the Symmetrix arrays that should not be auto-discovered.

Use the command 'SYMCLI\bin>symcfg list' to get the SymmID.

Note: Make sure that the provider is not running when you make the change. Delete the symapi_db.bin file and re-discover for the changes to take effect.

Q: Does the LocalDir/admin password expire?

A: Yes, it will expire after 90 days. EMC was not aware of this, and are looking into making it tunable in a future release. So as of 4.1 release, it will expire. If user resets password, it again expire in 90 days after resetting. If user creates new user, it will password expire in 90 days. You can change password from https://<ipaddress>:5989/ecomconfig

Q: Can I downgrade the 4.x.x provider down to 3.x.x?

A: If you uninstall the newest emc provider and install the 3.3.2 version you will have to delete the symapi_db.bin file. By not deleting the symapi_db.bi you will receive following error when running the dv command from the testsmiprovider.exe utility: "provider initialization error".

To downgrade, do the following:

1. Stop the Provider

2. Rename or delete the emc\symapi\db\symapi_db.bin file to <filename>.old

3. Start the Provider

4. Run TestSMIProvider and add your arrays.

Troubleshooting EMC Version Pre-4.0.0

Q: I want to monitor a Symmetrix V-Max Array. Which provider do I use?

A: Version 4.0 of the provider has added support for V-Max series. The provider is embedded with the array.

Q: What files are needed to send a bug to EMC?
A: Any issues related to the EMC provider, EMC requires the following info before they'll look into the problem:

All log files from <install_dir>\symapi\log

symapi_db.bin file, located <install_dir>\symapi\db

Output of the 'dv' command from the TestSmiProvider utility

Output of the 'tms' command from the TestSmiProvider utility

Q: How do I change the port the provider listens on?

A: To change the port, do the following:

On the machine running the Provider:

1. Stop the CIM Object Manager Service (see below how to stop provider)

2. edit C:\Program Files\EMC\SYMCLI\cimserver_planned.conf.

3. Change the http=5988 option to a port currently not in use.

4. Save the cimserver_planned.conf file.

Note: On unix systems make the changes in cimserver_planned.conf and cimserver_current.conf

5. Start the CIM Object Manager Service (see below on how to start provider)

6. In the Profiler GUI: Go to Administration > Hosts.

7. Click the monkey wrench icon for the Array.

8. Change the HTTP port to the port set in the cimserver_planned.conf on Provider.

9. Save the changes.

Q: How do I start/stop the provider from command prompt?

A: Windows:

1. Stop → <install_dir>SYMCLI/storbin/cimserver -stop emc_smi_provider

<install_dir>SYMCLI/storbin/stordaemon shutdown all

2. Start → <install_dir>SYMCLI/storbin/cimserver -start emc_smi_provider

Unix:

3. Stop → <install_dir>/SYMCLI/storbin/cimserver –s
4. Start → <install_dir>/SYMCLI/storbin/cimserver

Note: For solaris you MUST be in the <install_dir>/SYMCLI directory and run ./storbin/cimserver command

Q: Why does addsys time out when adding a CLARiiON, and how do I fix it?

A: This error typically comes from the cimserver.exe not running due to a bind exception on the default port (5988). To check if this is an issue, do the following:

1. Open the task manager to see if the cimserver.exe is running. If it is not, proceed.
2. Open the PegasusError.log located: C:\Program Files\EMC\SYMAPI\log.
3. Look for the following error:
   SEVERE cimserver: Could not bind: Bind failed: Failed to bind socket

Q: How do I reset EMC provider?

A: Please do the following to reset the EMC provider.

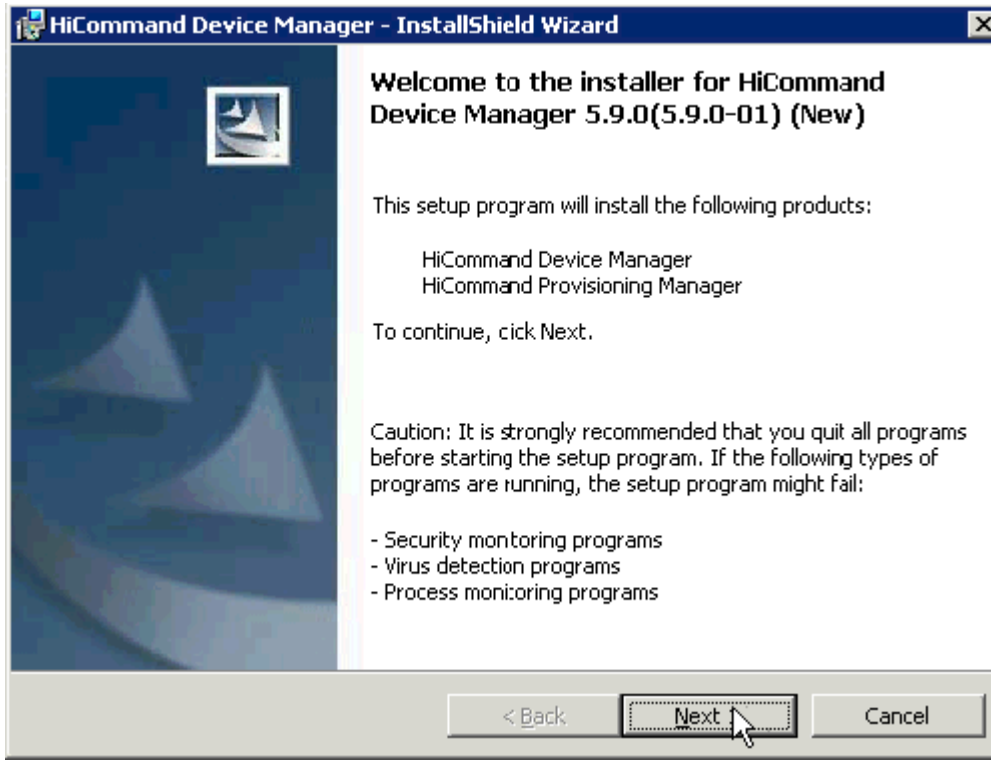
1. Stop the EMC provider (CIM Object Manager service).
2. Navigate to symapi\db directory (c:\Program Files\EMC\symapi\db).
3. Rename the symapi_db.bin file.
   NOTE: The provider will recreate the symap_db.bin file after it synchs itself with the array.
4. Start the EMC provider (CIM Object Manager service).
5. Follow the instructions in EMC > Adding A SAN section to add the array to be monitored by the provider.

Hitachi Data Systems (HDS) Provider

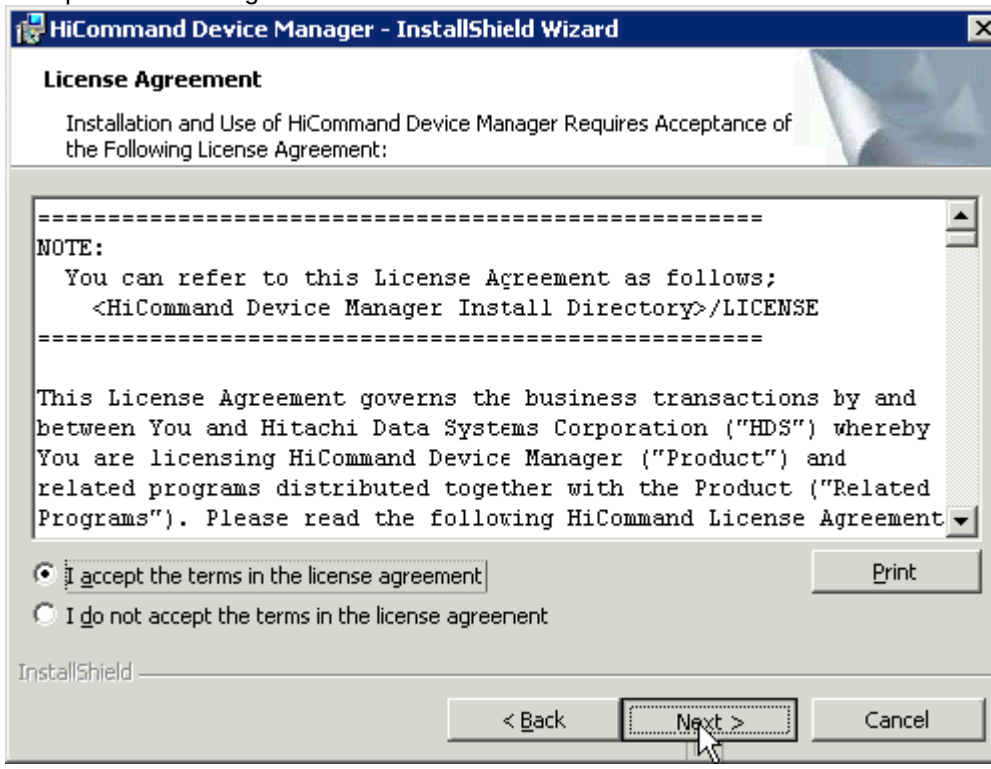
The following section detail installation steps for Windows. The HDS provider is part of the HiCommand Device Manager and is a purchased product.

Installation Steps:

1. Double click the HiCommand Device Manager Install package.
2. Click **Next** at the welcome screen.

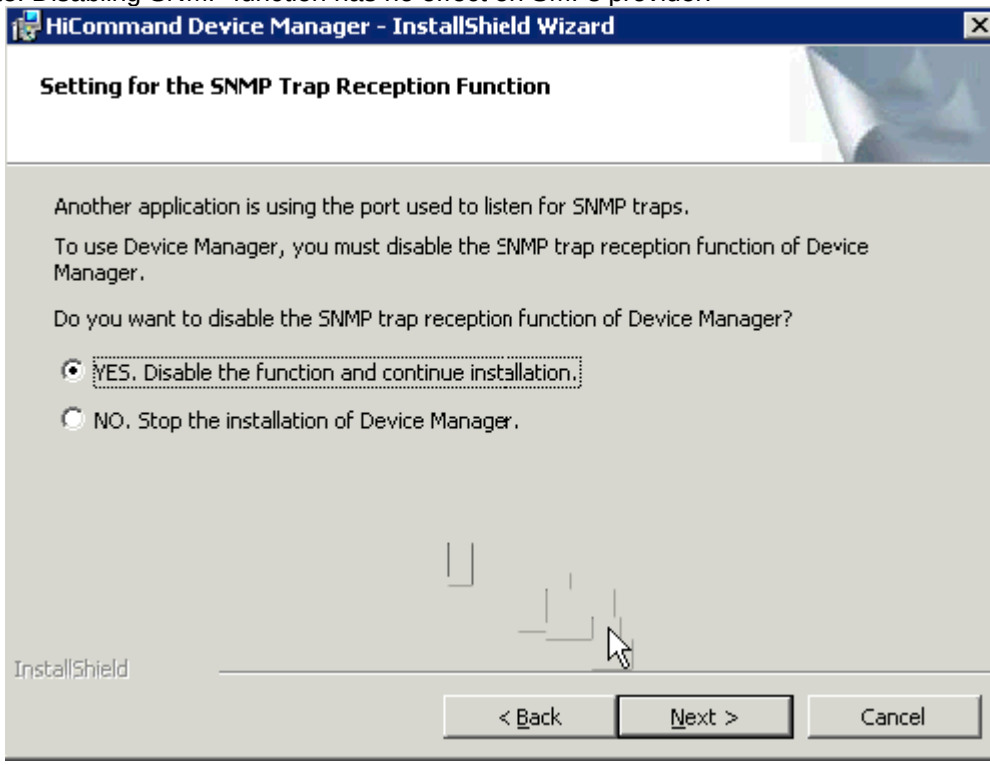

HiCommand Device Manager - InstallShield Wizard
Welcome to the installer for HiCommand Device Manager 5.9.0(5.9.0-01) (New)
This setup program will install the following products:
HiCommand Device Manager
HiCommand Provisioning Manager
To continue, cick Next.
Caution: It is strongly recommended that you quit all programs before starting the setup program. If the following types of programs are running, the setup program might fail:
- Security monitoring programs
- Virus detection programs
- Process monitoring programs
< Back
Next
Cancel

3. Accept the license agreement. Click **Next**.

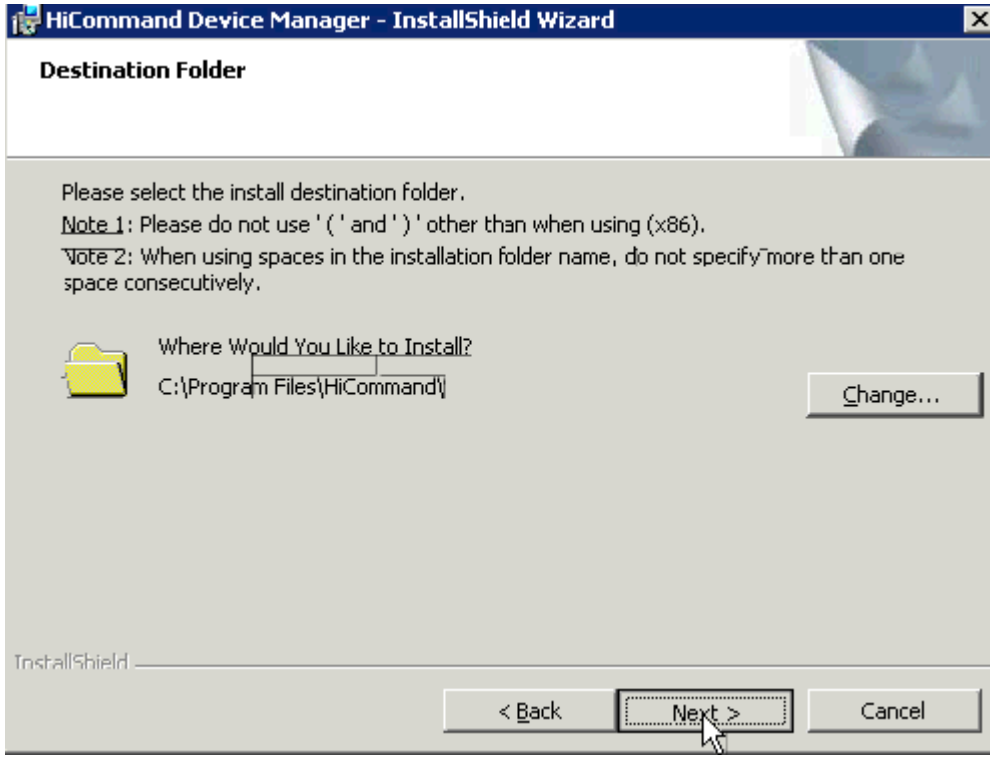

HiCommand Device Manager - InstallShield Wizard
License Agreement
Installation and Use of HiCommand Device Manager Requires Acceptance of the Following License Agreement:
==========
NOTE:
You can refer to this License Agreement as follows;
<HiCommand Device Manager Install Directory>/LICENSE
==========
This License Agreement governs the business transactions by and between You and Hitachi Data Systems Corporation ("HDS") whereby You are licensing HiCommand Device Manager ("Product") and related programs distributed together with the Product ("Related Programs"). Please read the following HiCommand License Agreement
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

4. Select Disable SNMP trap function if port 162 is in use. Otherwise, skip this step. Click **Next.**

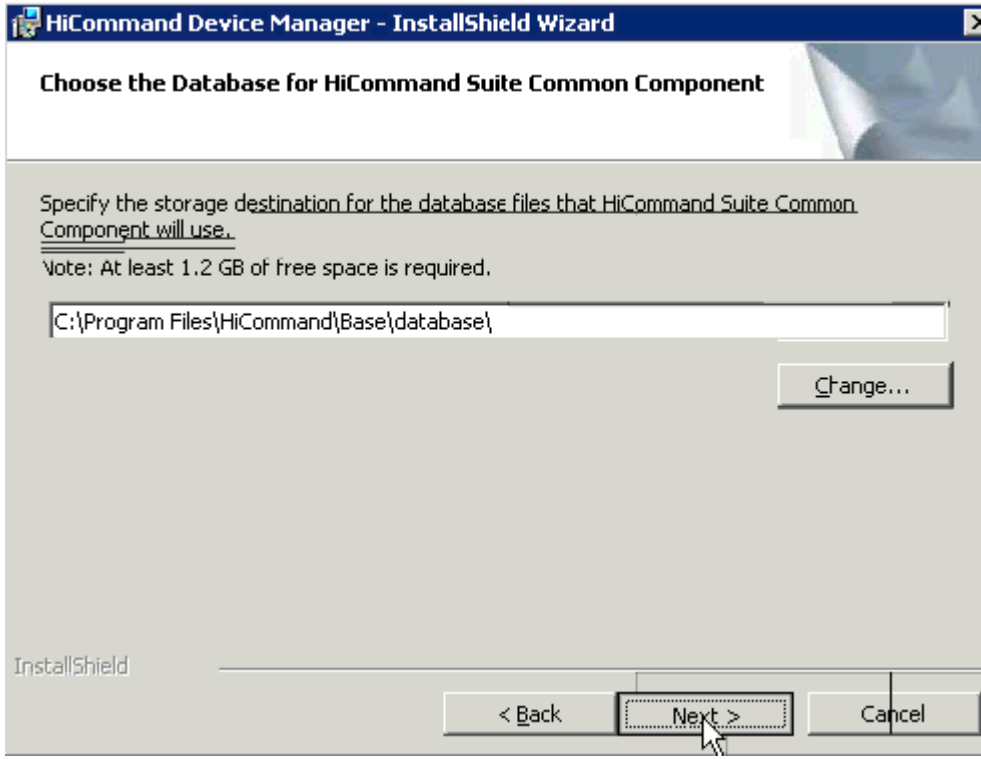
Note: Disabling SNMP function has no effect on SMI-s provider.


HiCommand Device Manager - InstallShield Wizard
Setting for the SNMP Trap Reception Function
Another application is using the port used to listen for SNMP traps.
To use Device Manager, you must disable the SNMP trap reception function of Device Manager.
Do you want to disable the SNMP trap reception function of Device Manager?
YES. Disable the function and continue installation.
NO. Stop the installation of Device Manager.
InstallShield
< Back
Next >
Cancel

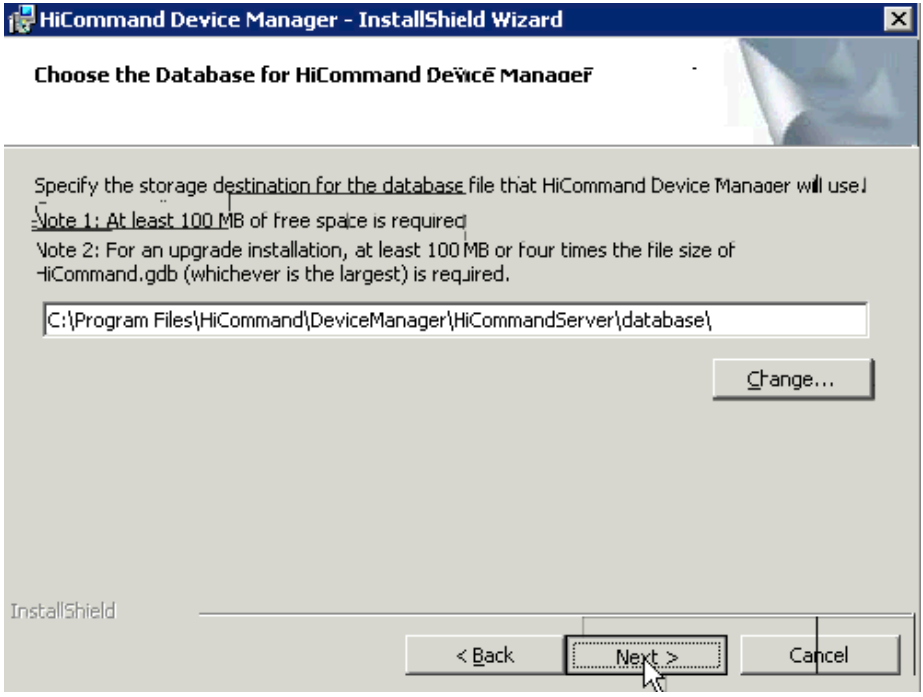
5. Choose the Destination folder for HiCommand. Click **Next**.


HiCommand Device Manager - InstallShield Wizard
Destination Folder
Please select the install destination folder.
Note 1: Please do not use ' (' and ') ' other than when using (x86).
Note 2: When using spaces in the installation folder name, do not specify more than one space consecutively.
Where Would You Like to Install?
C:\Program Files\HiCommand\
Change...
InstallShield
< Back
Next >
Cancel

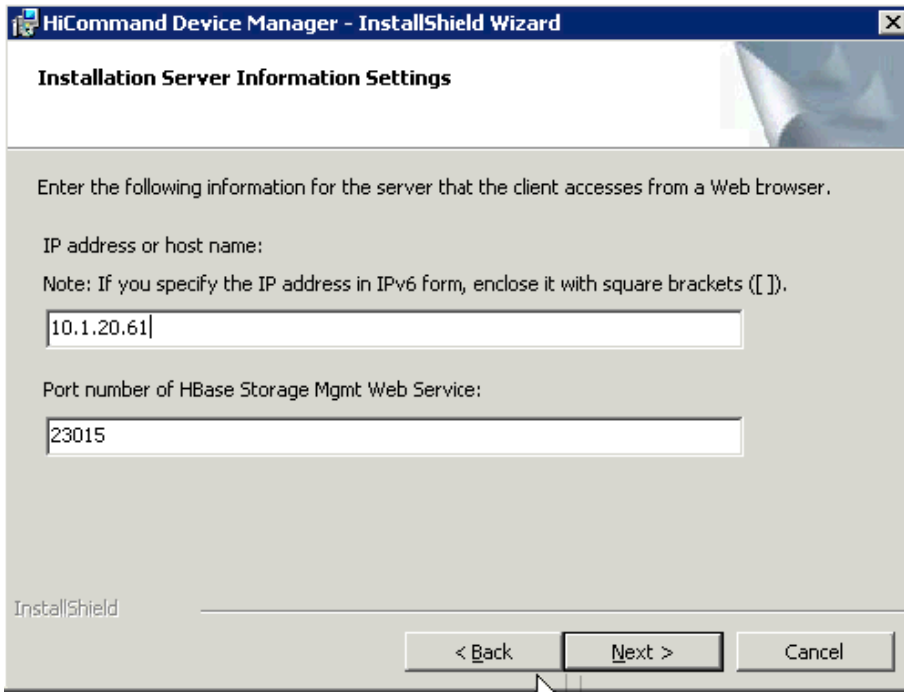
6. Choose the destination for the HiCommand Suite Common Component database. Click **Next.**


HiCommand Device Manager - InstallShield Wizard
Choose the Database for HiCommand Suite Common Component
Specify the storage destination for the database files that HiCommand Suite Common Component will use.
Note: At least 1.2 GB of free space is required.
C:\Program Files\HiCommand\Base\database\
Change...
InstallShield
< Back
Next >
Cancel

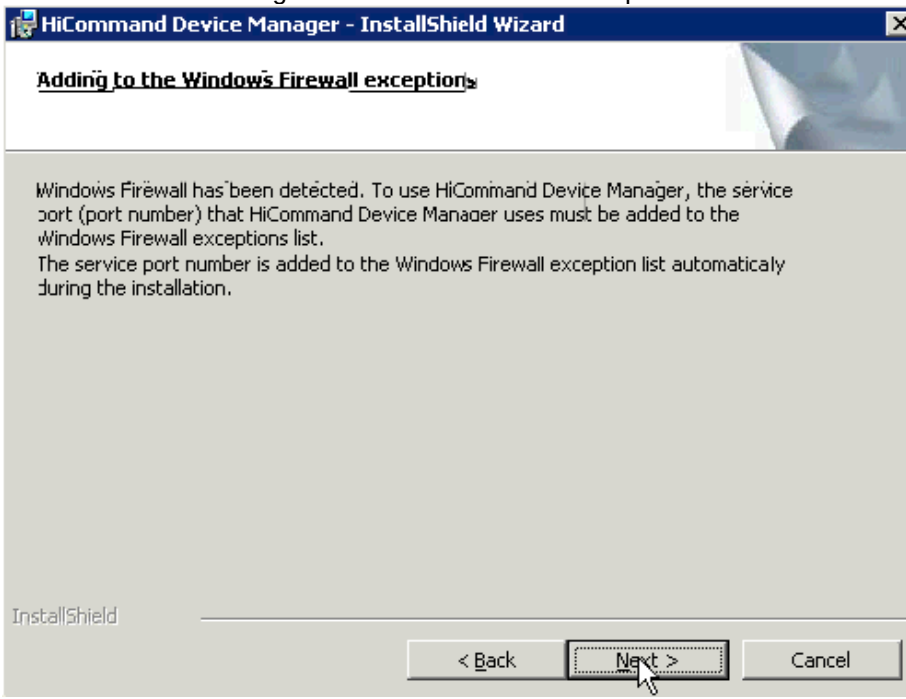
7. Choose the destination for the HiCommand Device manager database. Click **Next**.


HiCommand Device Manager - InstallShield Wizard
Choose the Database for HiCommand Device Manager
Specify the storage destination for the database file that HiCommand Device Manager will use.
Note 1: At least 100 MB of free space is required
Note 2: For an upgrade installation, at least 100 MB or four times the file size of HiCommand.gdb (whichever is the largest) is required.
C:\Program Files\HiCommand\DeviceManager\HiCommandServer\database\
Change...
InstallShield
< Back
Next >
Cancel

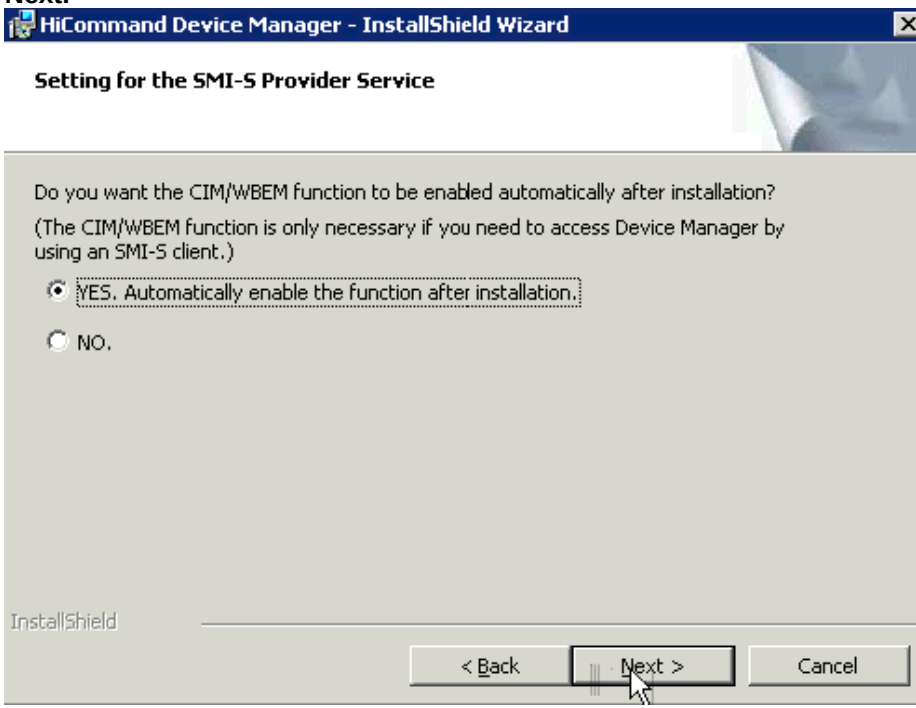
8. Specify the IP address of the machine HiCommand Device Manager is being installed on and Port for HBase Storage Management Web Service. Click **Next**.


HiCommand Device Manager - InstallShield Wizard
Installation Server Information Settings
Enter the following information for the server that the client accesses from a Web browser.
IP address or host name:
Note: If you specify the IP address in IPv6 form, enclose it with square brackets ([ ]).
10.1.20.61
Port number of HBase Storage Mgmt Web Service:
23015
InstallShield
< Back
Next >
Cancel

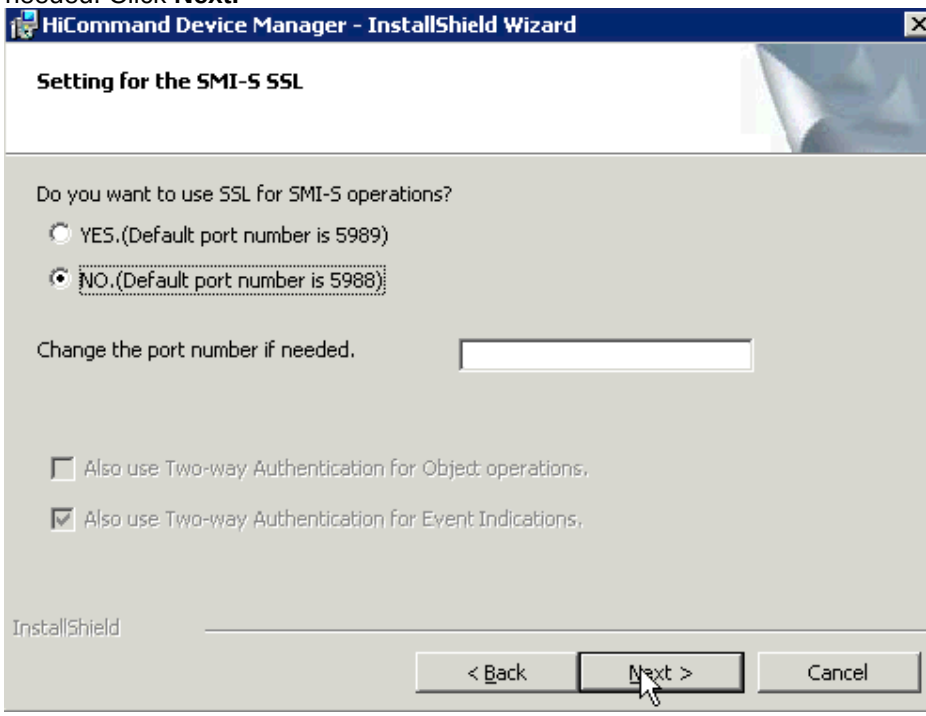
9. Click **Next** at the adding to the windows firewall exceptions screen.


HiCommand Device Manager - InstallShield Wizard
Adding to the Windows Firewall exceptions
Windows Firewall has been detected. To use HiCommand Device Manager, the service port (port number) that HiCommand Device Manager uses must be added to the Windows Firewall exceptions list.
The service port number is added to the Windows Firewall exception list automaticaly during the installation.
InstallShield
< Back
Next >
Cancel

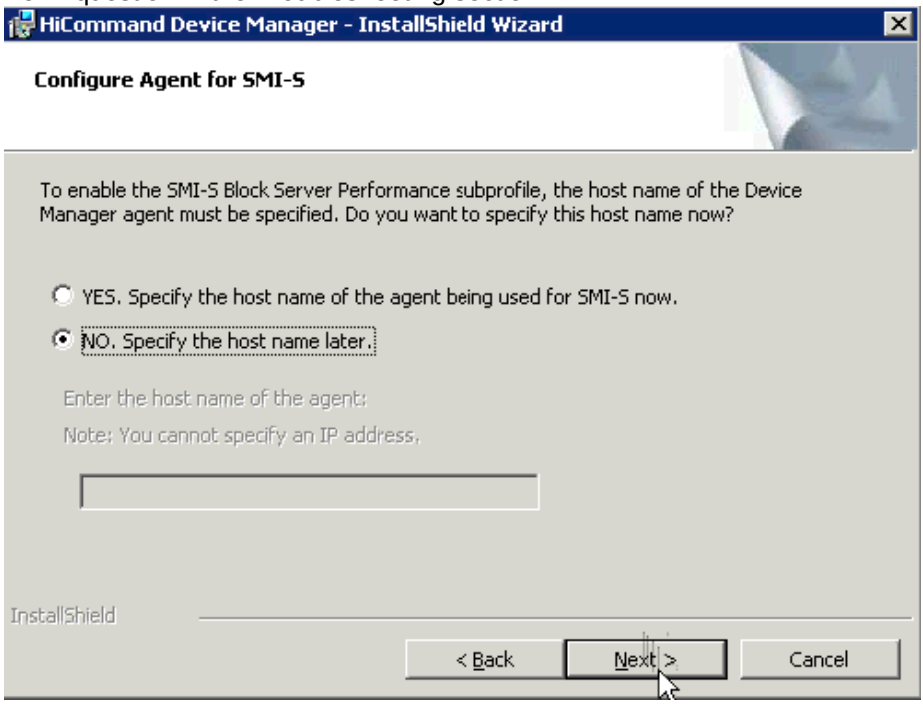
10. Select **YES** for enabling the SMI-s provider service after installation. Click **Next.**


HiCommand Device Manager - InstallShield Wizard
Setting for the SMI-S Provider Service
Do you want the CIM/WBEM function to be enabled automatically after installation?
(The CIM/WBEM function is only necessary if you need to access Device Manager by using an SMI-S client.)
YES. Automatically enable the function after installation.
NO.
InstallShield
< Back
Next >
Cancel

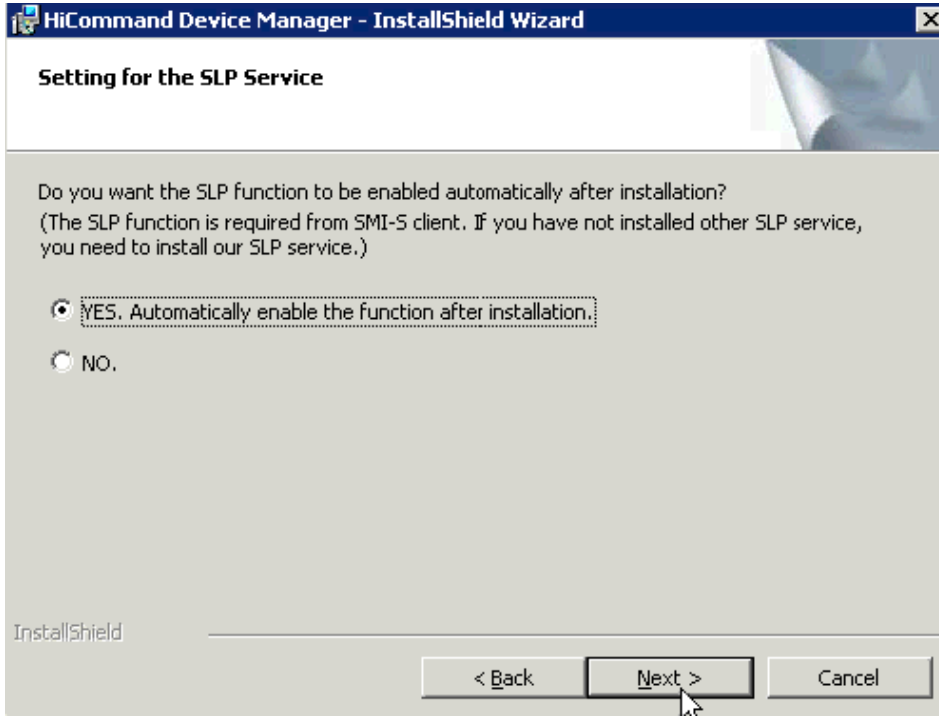
11. Select **NO** for SSL, unless a secure connection is needed. Change port if needed. Click **Next.**


HiCommand Device Manager - InstallShield Wizard
Setting for the SMI-S SSL
Do you want to use SSL for SMI-S operations?
YES.(Default port number is 5989)
NO.(Default port number is 5988)
Change the port number if needed.
Also use Two-way Authentication for Object operations.
Also use Two-way Authentication for Event Indications.
InstallShield
< Back
Next >
Cancel

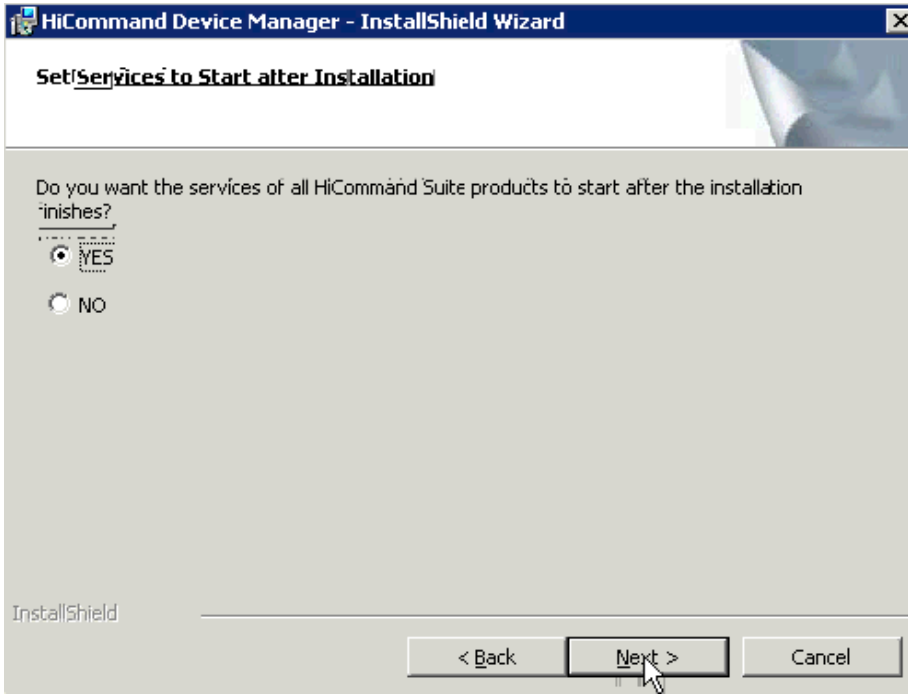
12. Depending on the Array type, a Device Manager agent may be needed. ***If it is needed, select yes and specify an IP address***. Refer to the “Which HDS arrays need a Device manager agent for performance metrics to be gathered from” question in the Troubleshooting section.


HiCommand Device Manager - InstallShield Wizard
Configure Agent for SMI-S
To enable the SMI-S Block Server Performance subprofile, the host name of the Device Manager agent must be specified. Do you want to specify this host name now?
YES. Specify the host name of the agent being used for SMI-S now.
NO. Specify the host name later.
Enter the host name of the agent:
Note: You cannot specify an IP address.
InstallShield
< Back
Next >
Cancel

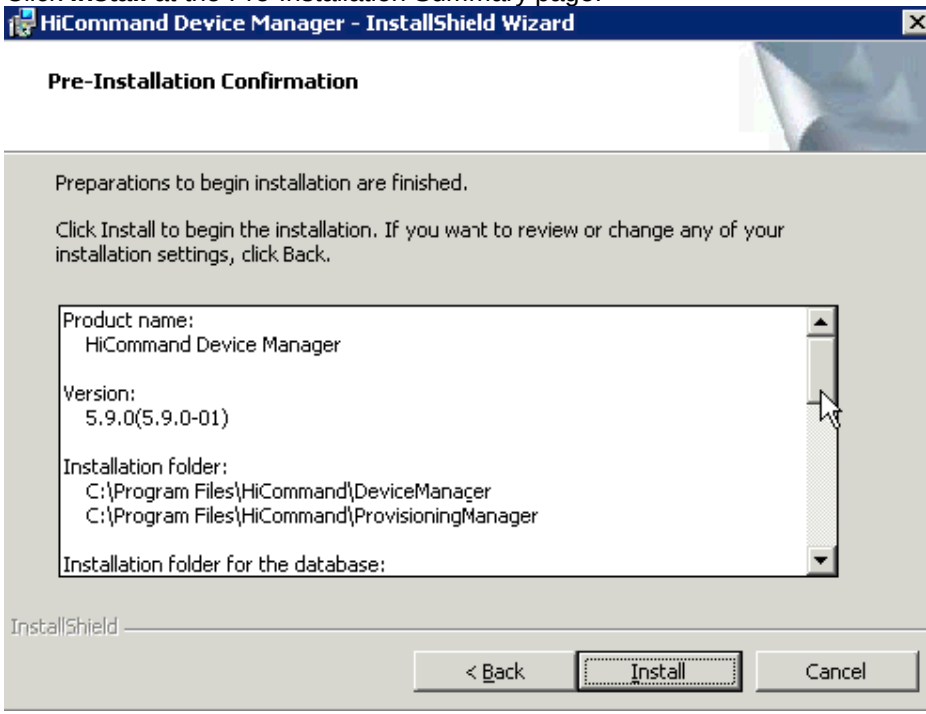
13. Select **YES** for the SLP function to be enabled after installation. Click **Next**.


HiCommand Device Manager - InstallShield Wizard
Setting for the SLP Service
Do you want the SLP function to be enabled automatically after installation?
(The SLP function is required from SMI-S client. If you have not installed other SLP service, you need to install our SLP service.)
YES. Automatically enable the function after installation.
NO.
InstallShield
< Back
Next >
Cancel

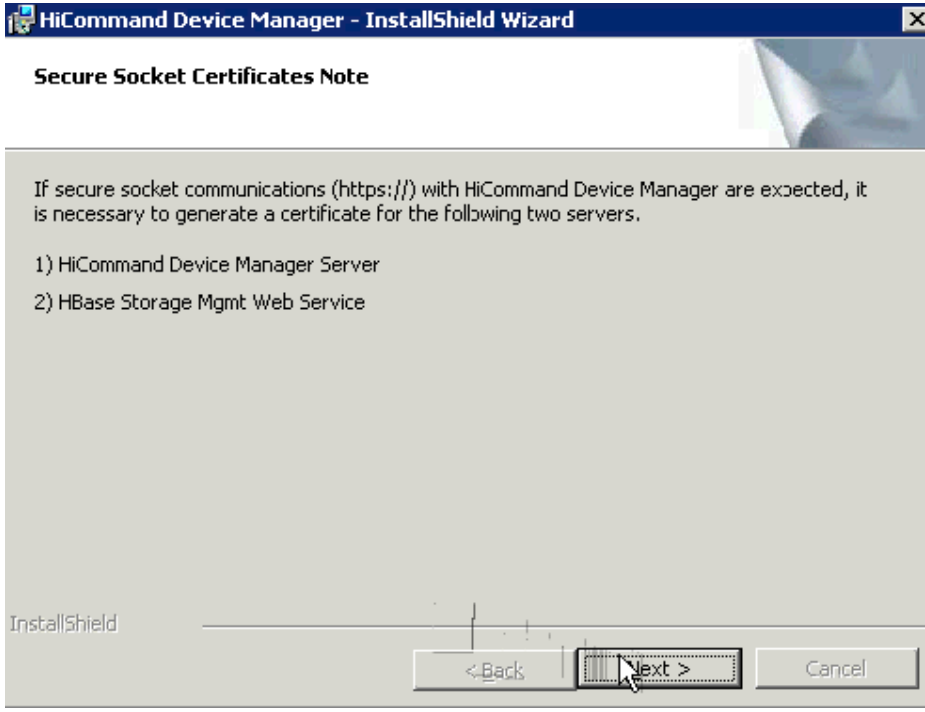
14. Select **YES** to start the HiCommand Suite to start after installation. Click **Next**.


HiCommand Device Manager - InstallShield Wizard
Set Services to Start after Installation
Do you want the services of all HiCommand Suite products to start after the installation finishes?
YES
NO
InstallShield
< Back
Next >
Cancel

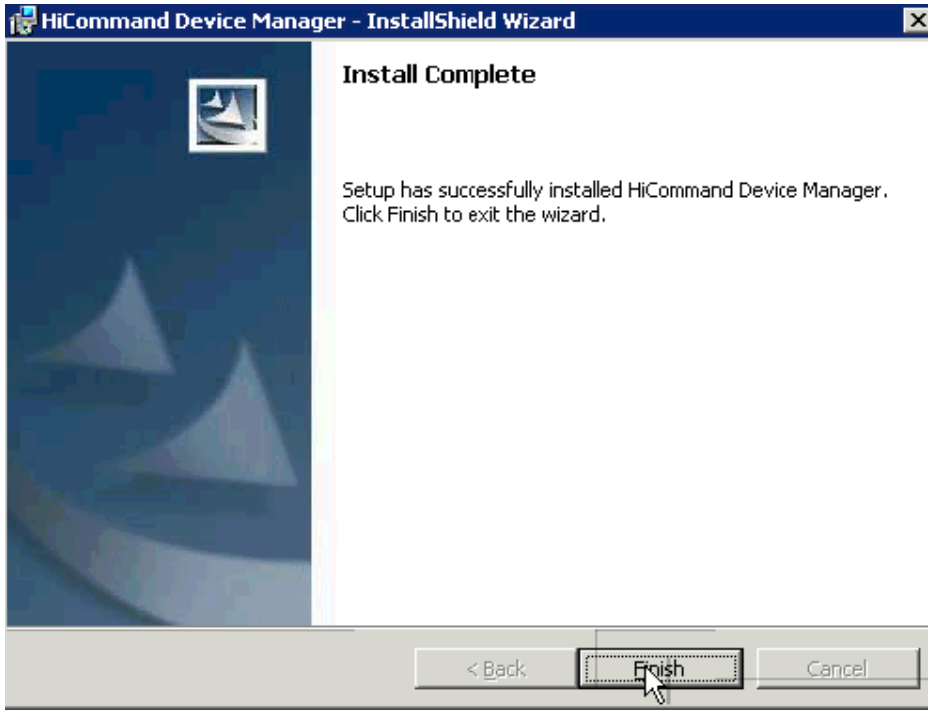
15. Click **Install** at the Pre-Installation Summary page.



16. Click **Next** at the Secure Socket Certificates Note.


HiCommand Device Manager - InstallShield Wizard
Secure Socket Certificates Note
If secure socket communications (https://) with HiCommand Device Manager are expected, it is necessary to generate a certificate for the following two servers.
1) HiCommand Device Manager Server
2) HBase Storage Mgmt Web Service
InstallShield
< Back
Next >
Cancel

17. Click **Finish**.



If you are using installing HDS 6.3 Device Manager

Q: How do I enable the provider?

A:

1.

EditC:\ProgramFiles\HiCommand\DeviceManager\HiCommandServer\config\server.properties

2. Edit following line and set server.cim.support to true

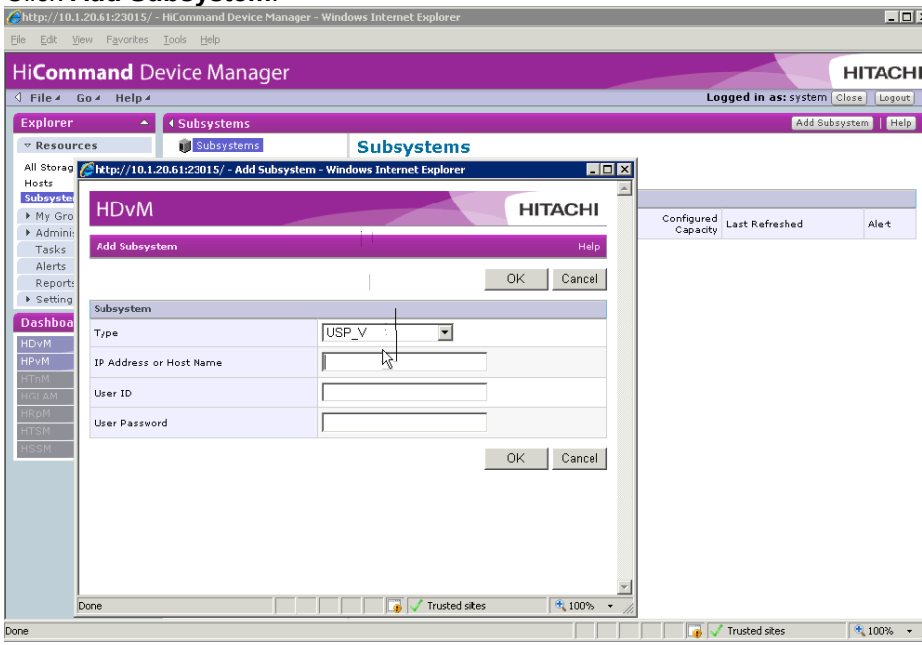
# whether the server supports CIM interface or not
server.cim.support=true

Adding a Subsystem

1. Open HiCommand Device Manager GUI.

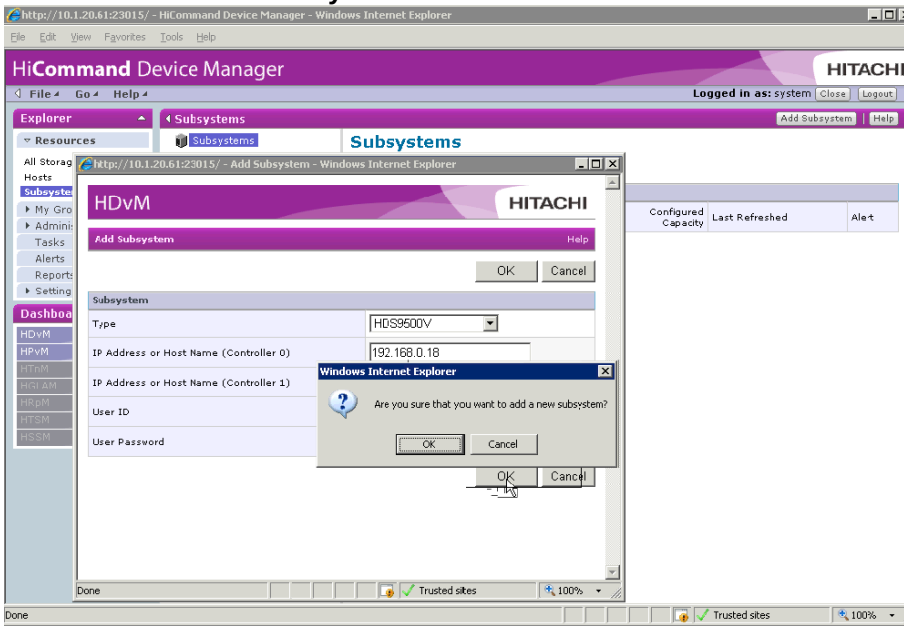
2. Click **Subsystems**.

3. Click **Add Subsystem**.

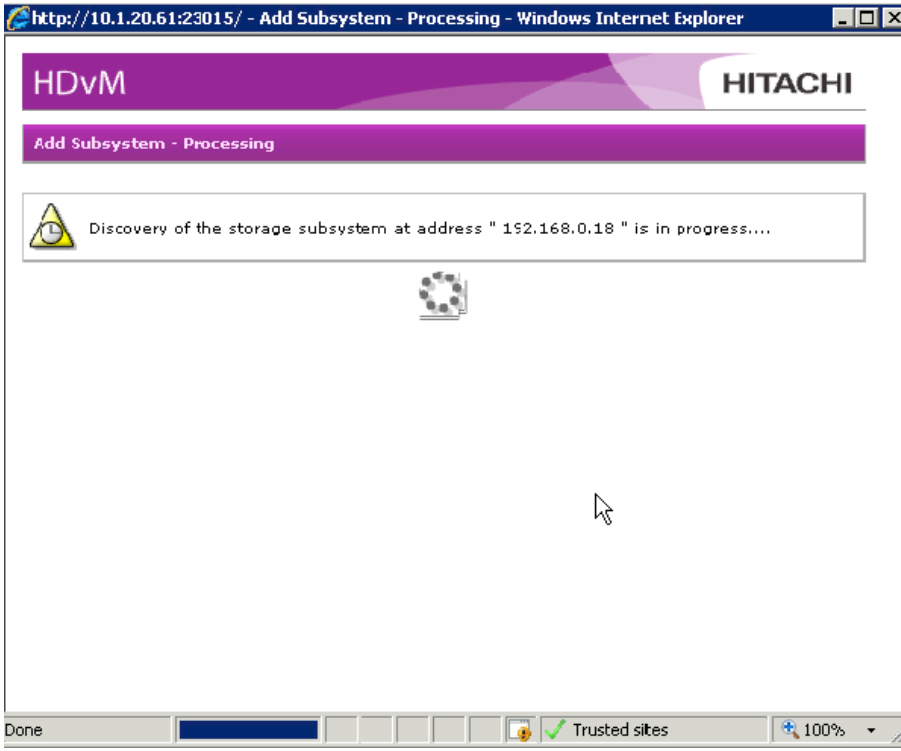


4. Select the Type of subsystem to be added.
5. Type in the IP Address of the Controllers.
6. Click **OK.**

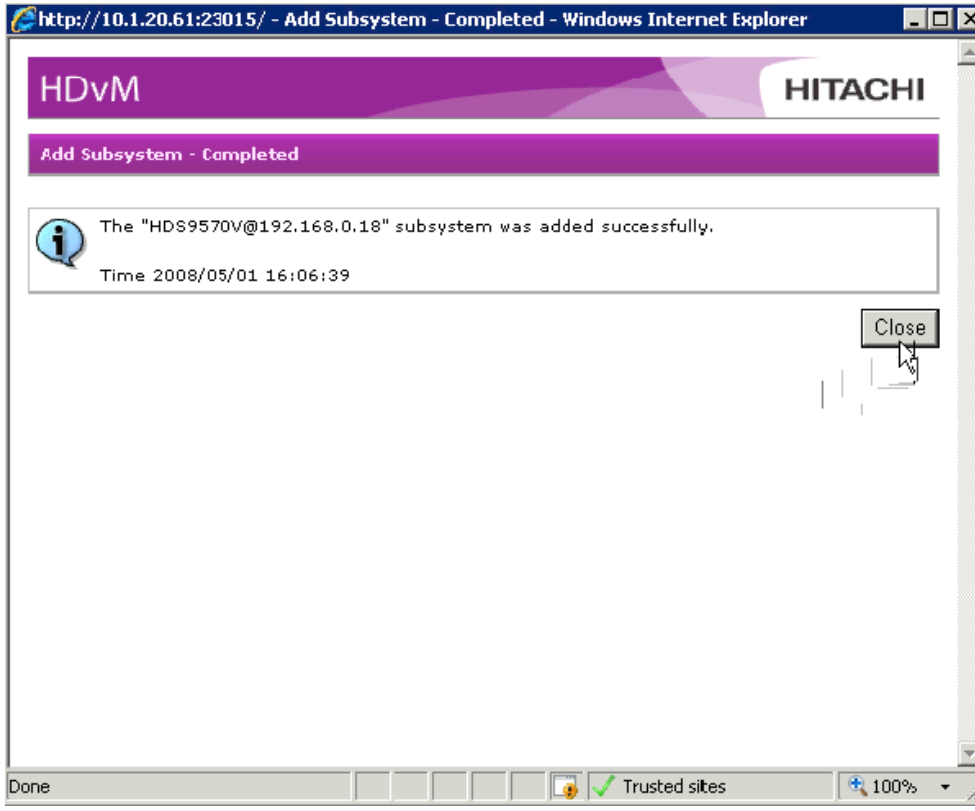
7. Click **OK** when asked “**Are you sure**”.



You should see:


http://10.1.20.61:23015/ - Add Subsystem - Processing - Windows Internet Explorer
HDvM
HITACHI
Add Subsystem - Processing
Discovery of the storage subsystem at address " 192.168.0.18 " is in progress....
Done
Trusted sites
100%

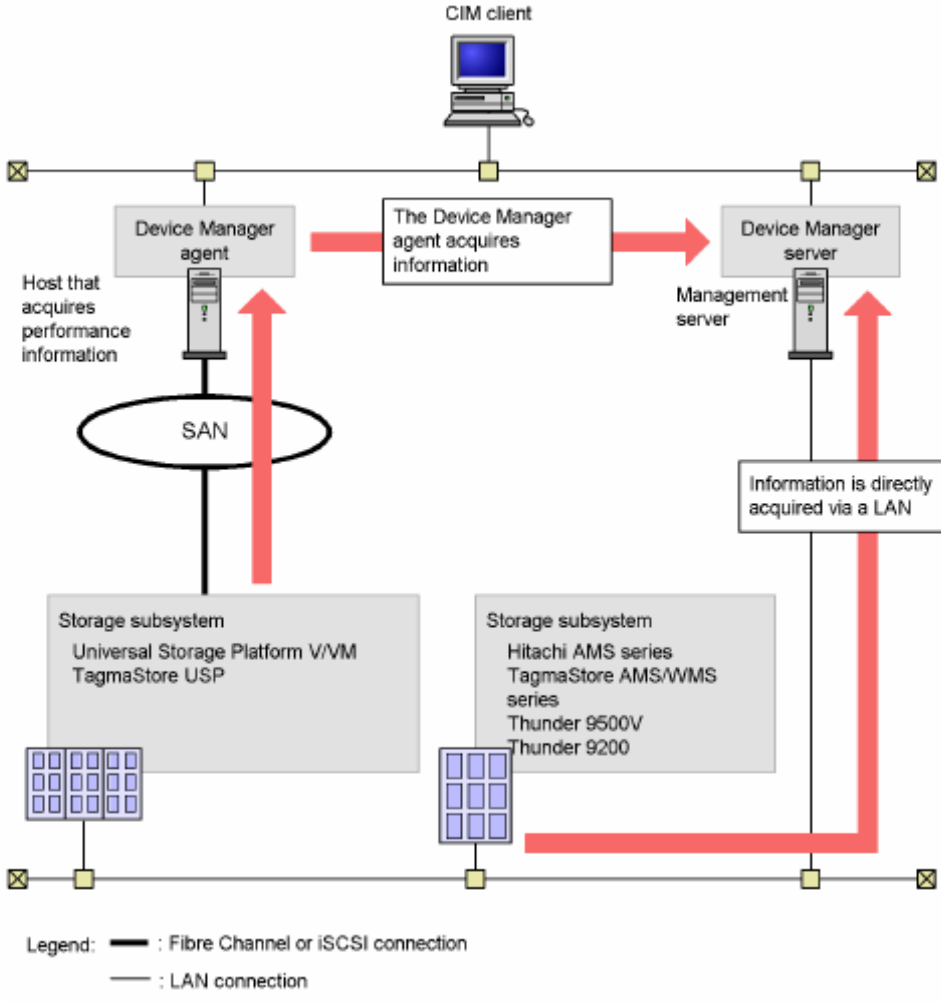
8. Click **Close**.



Troubleshooting HDS

The following section details troubleshooting steps for HDS.

Q: Which HDS arrays need a Device manager agent for performance metrics to be gathered from?
A: Refer to the following image (USP V/VM, and TagmaStor USP).



Q: What is the default username/password for the provider?

A: The username and password for the Provider is the same for the DataCenter (not administrator/administrator). If need be, they can create a new one for Profiler.

Q: What user permissions are required for the provider?

A: All resources with view privileges.

Q: What should I do if the test results window returns blank and I am using an admin ID to access the device manager?

A: Save the resource and check the SMI-S module log. If you see an Access denied error this means that the ID you are using doesn't have the proper permissions. Use the **ID:** System and **Password:** manager (both are case sensitive). This should solve your problem.

Q. How do I enable performance statistics?

A:

To enable performance on a USP/USP-v/USP-vm series storage system:

There are two pieces of software that have to be installed on the command view(in case of HP XP)/device manager server.

1. Hitachi/XP Raid Manager software which is only needed to create the device library.
2. Device Manager agent which can access the command device to transfer the performance data. Device Manager agent requires the Hitachi/XP Raid Manager device library to function.

The system that Device Manager/Command View is running on must have SAN access to the command device.

Follow the instructions to install the XP Raid Manager, but you do not need to actually have the HORCM process running.

For further information see the XP Command View Advanced Edition software server administrator guide for Device Manager and Provisioning Manager (in case HP XP) or Hitachi Storage Command Suite Software Server Installation and Configuration Guide for Hitachi Device Manager and Provisioning Manager

To enable performance on a AMS/WMS/Thunder 9500v/Thunder 9200 series storage system:

See the XP Command View Advanced Edition software server administrator guide for Device Manager and Provisioning Manager (in case HP XP) or Hitachi Storage Command Suite Software Server Installation and Configuration Guide for Hitachi Device Manager and Provisioning Manager

Q: What is the minimum provider version to get performance statistics?

A: Provider version must be High Command Device Manager 5.9 or later.

Q: What performance metrics are available?

A: Volume, port, and overall array performance metrics.

Q: Will disk or controller performance be available?

A: No. HDS does not plan to support those metrics via smi-s.

Q: Is performance supported on all arrays?

A: No. Performance is not available on the Lightning series arrays (9900, 9900-v).

NOTE: The Lightning series is obsolete and replaced by AMS/WMS.

Q: How do I enable performance on 9580?

A: Perform following steps:

1. Start Storage Navigator
2. Change the operation mode to Management Mode
3. Selected Performance tab from Settings-->Configuration Settings menu.
4. Select the Performance Statistics tab.
5. Check all performance choices

Q: What is the difference between Tagma Store and USP?

A: Tagma Store is an outdated name, and has since been replaced with USP naming convention.

Storage System	HDS Models	Rebranded HP Models	Rebranded SUN Models
Lightning 9900	9910, 9960	XP48, XP512	
Lightning 9900-V	9970V, 9980V	XP128, XP1024	
USP-V	R600, R601	XP20000, XP24000	9990V
USP	USP100, USP600, USP1100, NSC55	XP10000, XP12000, SVS200	
Thunder 9500-V	9520V, 9530V, 9570V, 9580V		
9200	9200, 9200L		
AMS	AMS200, AMS500, AMS1000,		

	AMS2100, AMS2300, AMS2500		
WMS	WMS100		
SMS	SMS100		

Note:

Midrange arrays:
9200 (thunder)
9500 (thunder)
9900, 9900-v (Lightning – obsolete and replaced by AMS, WMS)
AMS, WMS (replacement for above 9900 series)

Enterprise
USP 100, USP 600, USP 1100, NSC (1st generation arrays)
USP-V, USP-VM (2nd generation)

Q: What is the command for getting the Hdvm data base and logs dump?

A:

1. Go to the High Command installation directory from a command prompt.

For Example:

On Windows : C:\Program Files\HiCommand\Base\bin

On Solaris/Linux : /opt/HiCommand/Base/bin

2. Run the command below:

hcmdsgetlogs /dir <empty-directory-where-to-keep-the-dump> /arc <archive-file-name>

For Example:

hcmdsgetlogs /dir C:\logs_work /arc hicmd_log

In this case the dump will be in the directory C:\logs_work.

Note: User needs administrator privilege on the system to run this command.

Q: How do I change the memory settings for Device Manager?

A: Steps to change the memory settings - from "Device Manager Server Installation and Configuration Guide"

3.1.2.3 Setting Memory Heap Size When Using CIM/WBEM

If CIM/WBEM functions are being used, you might have to increase the memory heap size of the Device Manager server, depending on the conditions.

Note: that the required memory heap size differs depending on the CIM client you are using.
To change the memory heap size:

1. Use a text editor to open the following file:
2. Installation-folder-for-the-Device-Manager-server\HiCommandServer\Server.ini
3. Change the value of JVM_XOPT_HEAP_MAX to new-setting-value (units: MB), which is
   calculated by using the two formulas below.

The format is as follows:
JVM_XOPT_HEAP_MAX = -Xmxnew-setting-valuem
calculation-value-for-SMI-S-Provider = 30,000 x number-of-LDEVs x number-ofpaths- per-LDEV / 1048576

If the value of number-of-paths-per-LDEV becomes less than 1, assume that this value is equal to 1 for the calculation.

The value of calculation-value-for-SMI-S-Provider is expressed in megabytes. Round this value up to the nearest whole number.

If this value is less than 256 (MB), assume that it is equal to 256 for the calculation. new-setting-value = current-setting-value + calculation-value-for-SMI-S-Provider

All of the values in the above formula are expressed in megabytes. The value of new-setting-value obtained from the above formula is the memory heap size required for obtaining the class information that belongs to the bottom layer in a CIM class.

When an upper-layer class is specified, some SMI-S clients might obtain information of all the classes below that class at the same time. In this case, required capacity will be larger than the value of new-setting-value obtained from this formula.

Restart the Device Manager server as follows:

Select Start, Programs, HiCommand, Device Manager, and then Stop Server. After the Device Manager server has stopped, select Start, Programs, HiCommand, Device Manager, and then Start Server.

Q: How do I enable SMI-S on Device Manager if I didn't enable during installation?

A: Edit the file Program Files\HiCommand\DeviceManager\HiCommandServer\config and change from server.cim.support=false to server.cim.support=true. Restart HiCommand Device Manager service.

HP Providers

The HP Provider is an installable option with Command View. If it is not selected during install, you can either run the Command View install again from CD (the install will detect that SMI-S was not selected) or Download and install the SMI-S provider from the HP website.

Download: http://h18006.www1.hp.com/storage/smis.html

Compatibility Matrix: http://h18006.www1.hp.com/storage/smis-matrix.html

Reference Guides: http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&cc=us&taskId=101&prodClassId=-1&contentType=SupportManual&docIndexId=64180&prodTypeId=18964&prodSeriesId=471497

HP Provider Installation

The following section details the installation of various versions of the HP Provider.

HP XP Provider

The HP XP provider is actually an Hitachi re-branded array. For more information refer to the "Hitachi Data Systems (HDS) Provider" section on page "179".

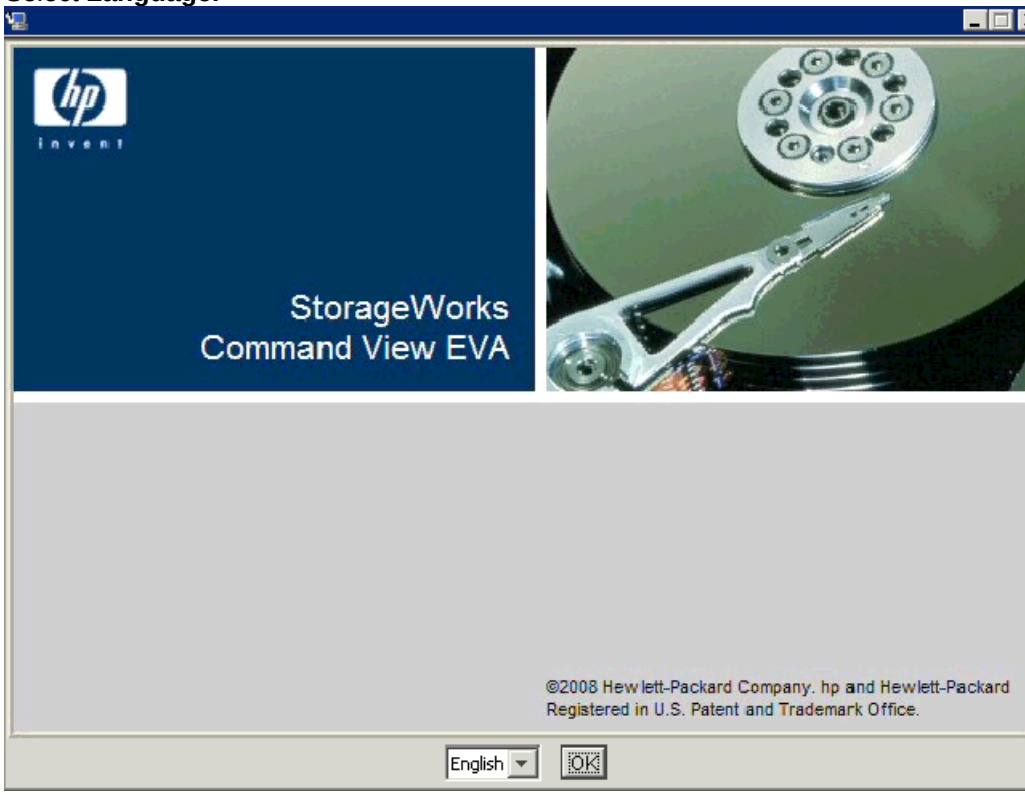
HP EVA Provider (Command View)

The following section details the installation on a Windows server.

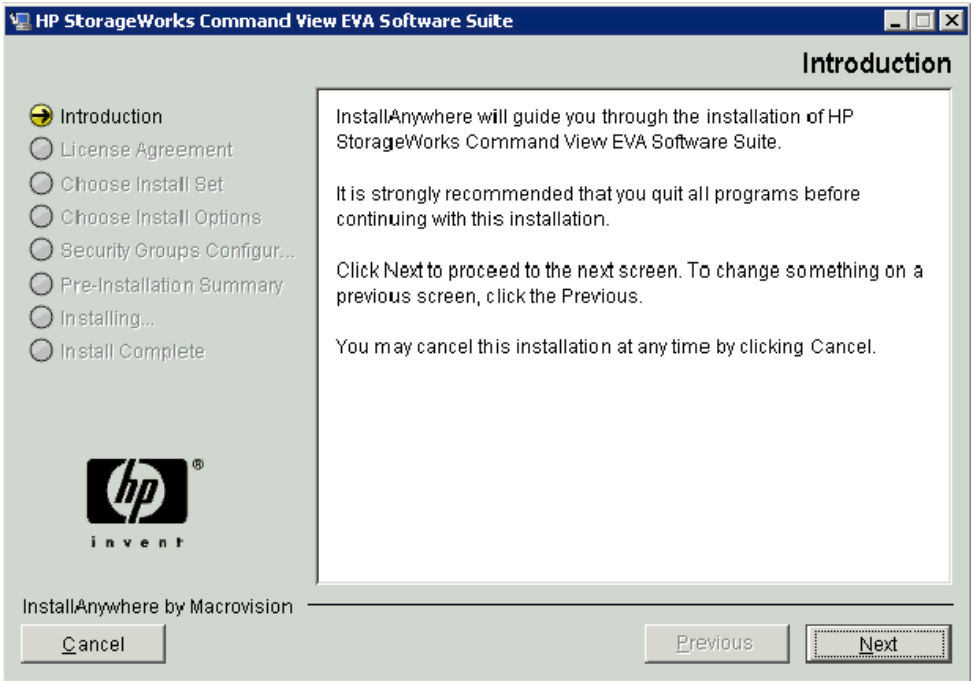
Windows install:

Double click the setup for Command View 8.

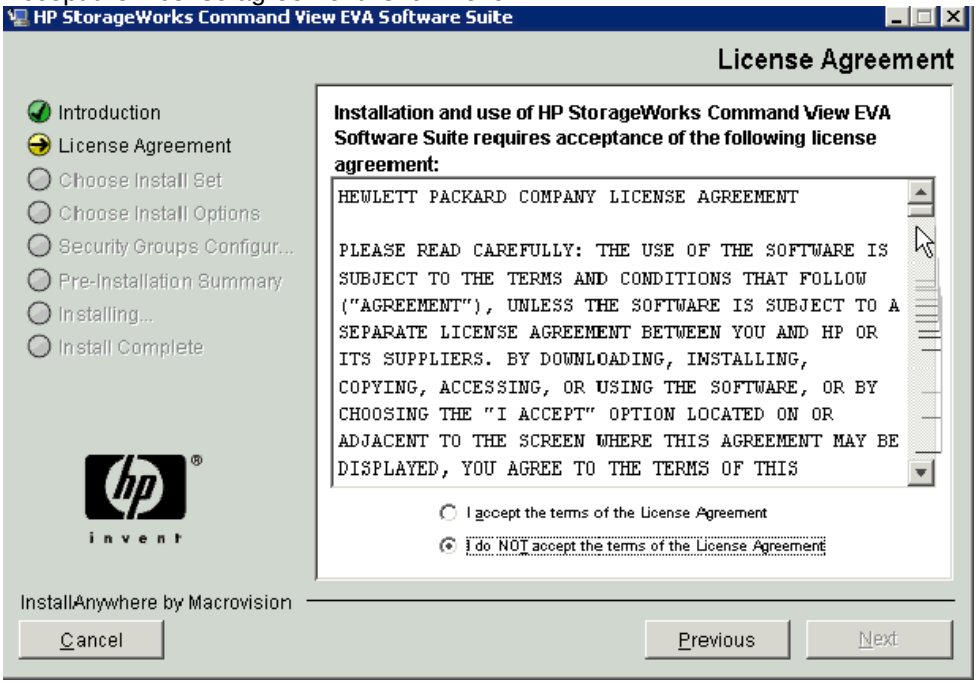
Select **Language.**



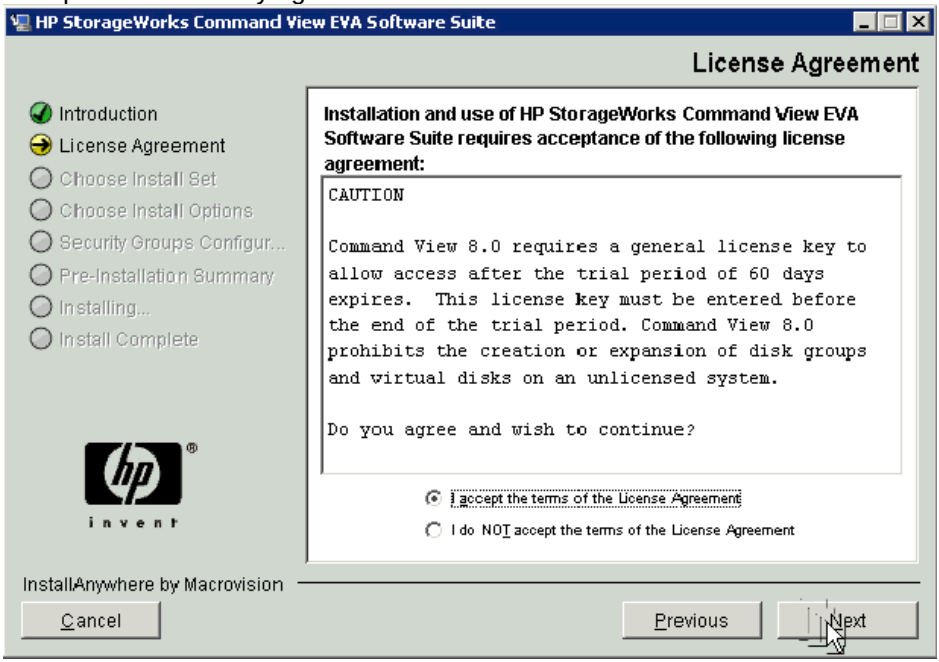
Click **Next** at the introduction screen.


HP StorageWorks Command View EVA Software Suite
Introduction
Introduction
License Agreement
Choose Install Set
Choose Install Options
Security Groups Configur...
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere will guide you through the installation of HP StorageWorks Command View EVA Software Suite.
It is strongly recommended that you quit all programs before continuing with this installation.
Click Next to proceed to the next screen. To change something on a previous screen, click the Previous.
You may cancel this installation at any time by clicking Cancel.
invent
InstallAnywhere by Macrovision
Cancel
Previous
Next

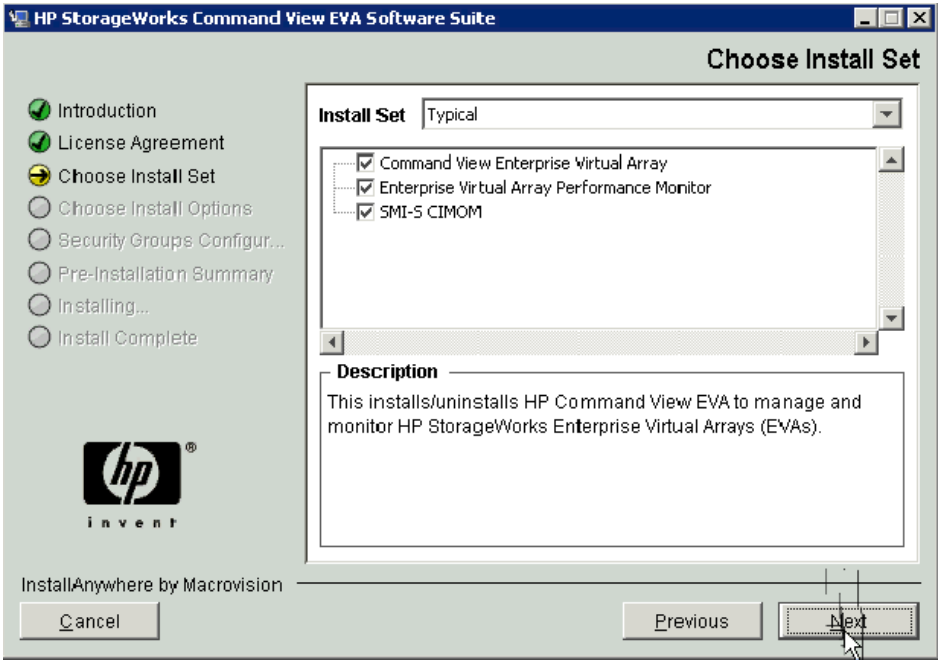
Accept the License agreement. Click **Next.**


HP StorageWorks Command View EVA Software Suite
License Agreement
Introduction
License Agreement
Choose Install Set
Choose Install Options
Security Groups Configur...
Pre-Installation Summary
Installing...
Install Complete
Installation and use of HP StorageWorks Command View EVA Software Suite requires acceptance of the following license agreement:
HEWLETT PACKARD COMPANY LICENSE AGREEMENT
PLEASE READ CAREFULLY: THE USE OF THE SOFTWARE IS SUBJECT TO THE TERMS AND CONDITIONS THAT FOLLOW ("AGREEMENT"), UNLESS THE SOFTWARE IS SUBJECT TO A SEPARATE LICENSE AGREEMENT BETWEEN YOU AND HP OR ITS SUPPLIERS. BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE SOFTWARE, OR BY CHOOSING THE "I ACCEPT" OPTION LOCATED ON OR ADJACENT TO THE SCREEN WHERE THIS AGREEMENT MAY BE DISPLAYED, YOU AGREE TO THE TERMS OF THIS
I accept the terms of the License Agreement
I do NOT accept the terms of the License Agreement
invent
InstallAnywhere by Macrovision
Cancel
Previous
Next

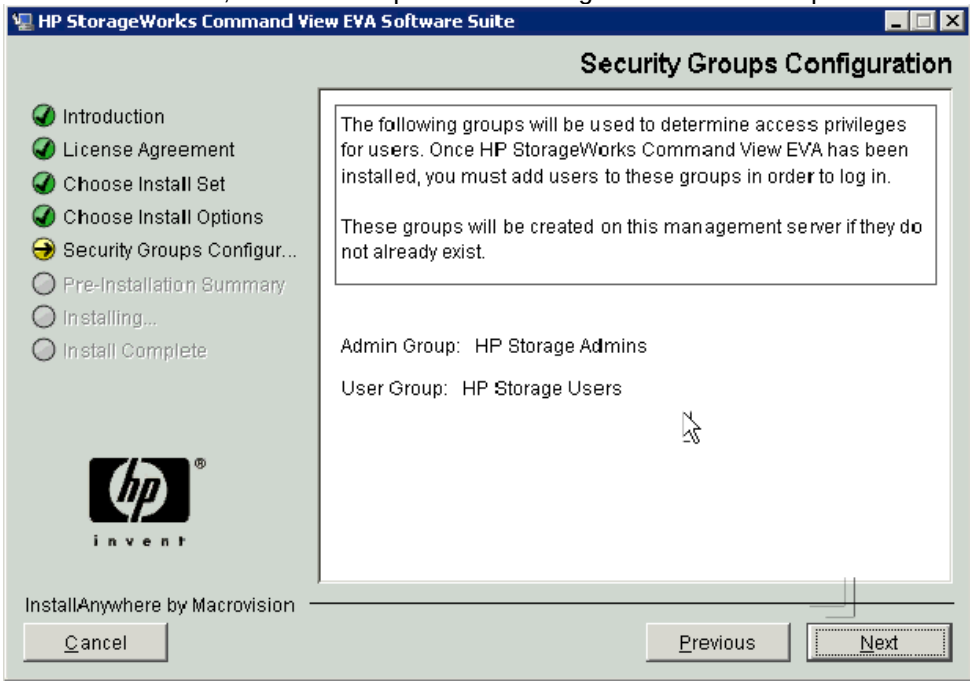
Accept the license key agreement. Click **Next**.


HP StorageWorks Command View EVA Software Suite
License Agreement
Introduction
License Agreement
Choose Install Set
Choose Install Options
Security Groups Configur...
Pre-Installation Summary
Installing...
Install Complete
Installation and use of HP StorageWorks Command View EVA Software Suite requires acceptance of the following license agreement:
CAUTION
Command View 8.0 requires a general license key to allow access after the trial period of 60 days expires. This license key must be entered before the end of the trial period. Command View 8.0 prohibits the creation or expansion of disk groups and virtual disks on an unlicensed system.
Do you agree and wish to continue?
I accept the terms of the License Agreement
I do NOT accept the terms of the License Agreement
invent
InstallAnywhere by Macrovision
Cancel
Previous
Next

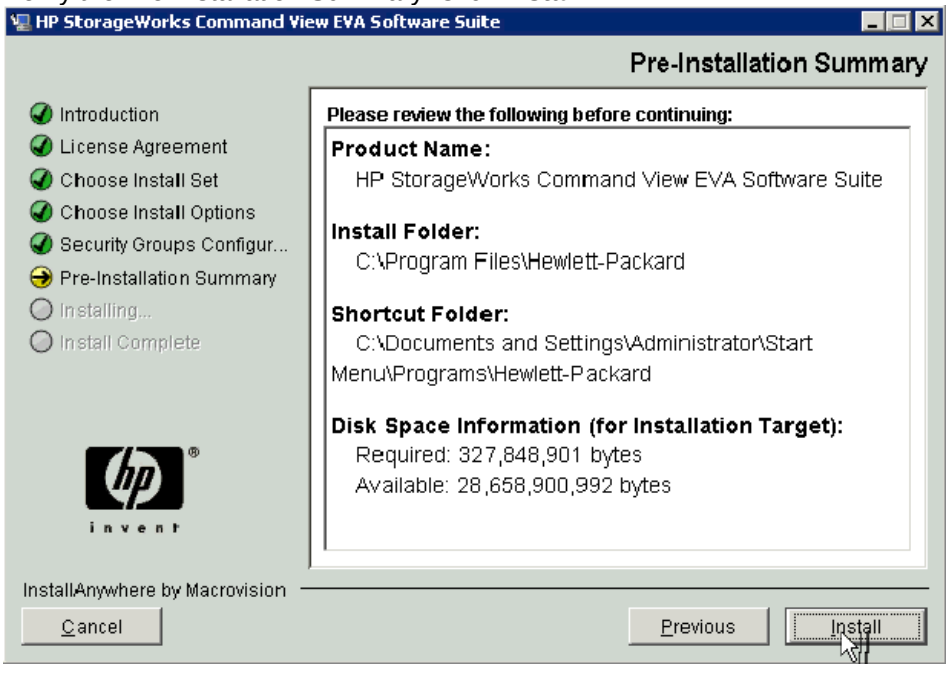
Choose Install Set. Check EVA PerfMon and SMI-S Cimom. Click **Next.**



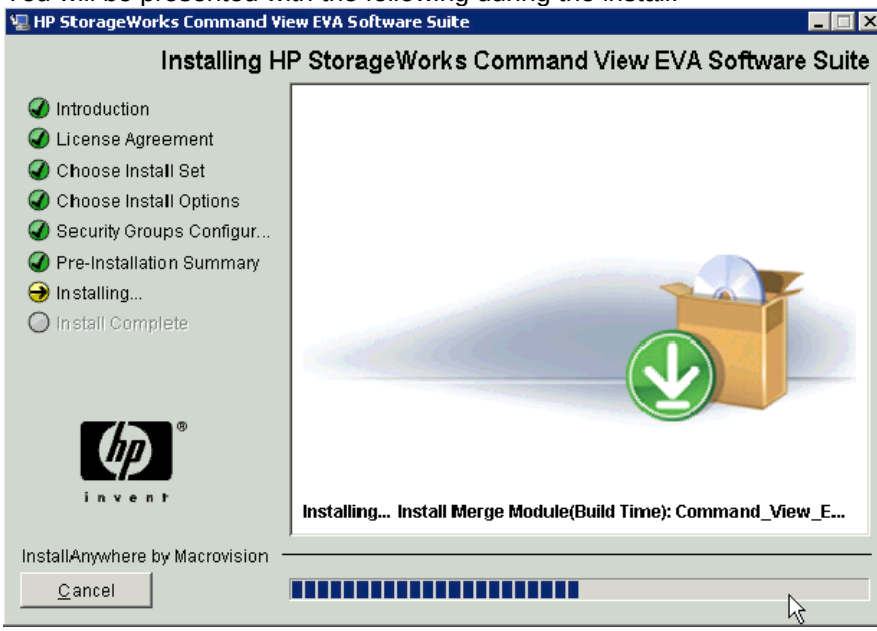
Keep in mind the Security Groups Configuration for post installation. Click **Next**.
NOTE: Post install, follow the steps in the “Adding Users to HP Groups” section.


HP StorageWorks Command View EVA Software Suite
Security Groups Configuration
Introduction
License Agreement
Choose Install Set
Choose Install Options
Security Groups Configur...
Pre-Installation Summary
Installing...
Install Complete
The following groups will be used to determine access privileges for users. Once HP StorageWorks Command View EVA has been installed, you must add users to these groups in order to log in.
These groups will be created on this management server if they do not already exist.
Admin Group: HP Storage Admins
User Group: HP Storage Users
invent
InstallAnywhere by Macrovision
Cancel
Previous
Next

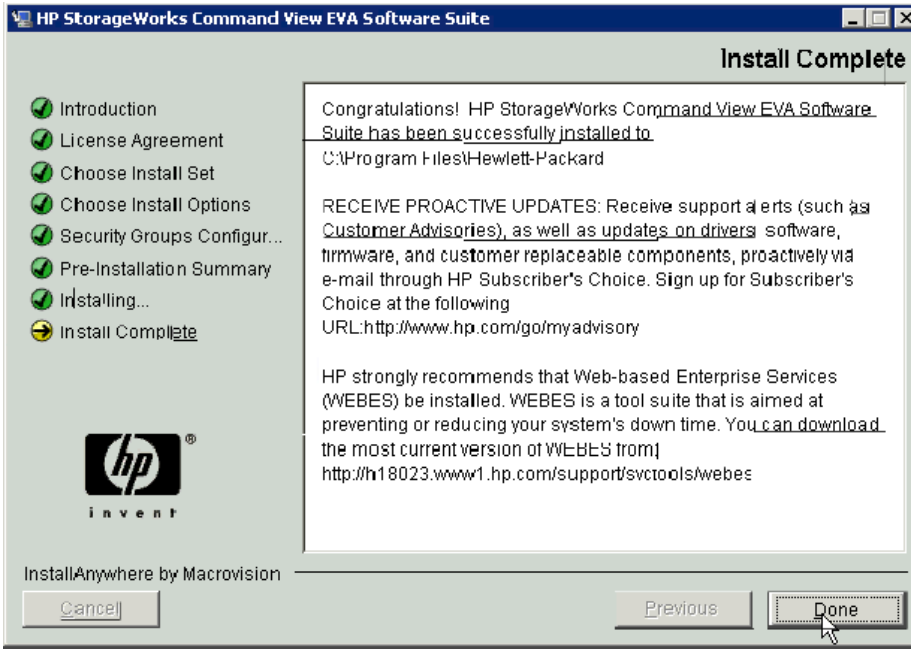
Verify the Pre-Installation Summary. Click **Install**.



You will be presented with the following during the install.



Click **Done**.

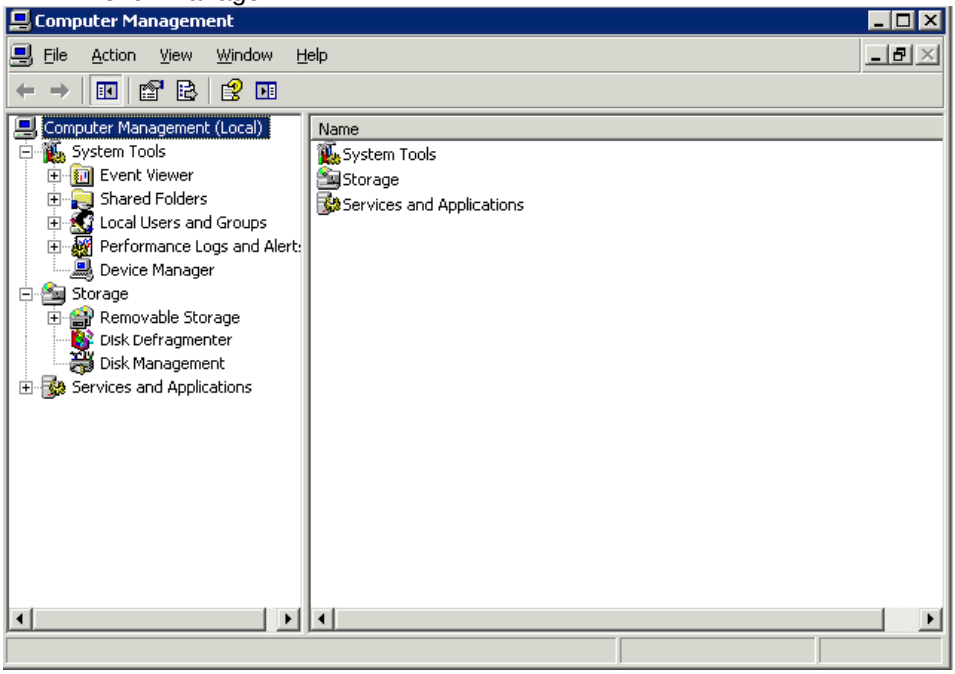

HP StorageWorks Command View EVA Software Suite
Install Complete
Introduction
License Agreement
Choose Install Set
Choose Install Options
Security Groups Configur...
Pre-Installation Summary
Installing...
Install Complete
invent
Congratulations! HP StorageWorks Command View EVA Software Suite has been successfully installed to
C:\Program Files\Hewlett-Packard
RECEIVE PROACTIVE UPDATES: Receive support alerts (such as Customer Advisories), as well as updates on drivers, software, firmware, and customer replaceable components, proactively via e-mail through HP Subscriber's Choice. Sign up for Subscriber's Choice at the following
URL:http://www.hp.com/go/myadvisory
HP strongly recommends that Web-based Enterprise Services (WEBES) be installed. WEBES is a tool suite that is aimed at preventing or reducing your system's down time. You can download the most current version of WEBES from
http://h18023.www1.hp.com/support/svctools/webes
InstallAnywhere by Macrovision
Cancel
Previous
Done

Adding Users to HP Groups

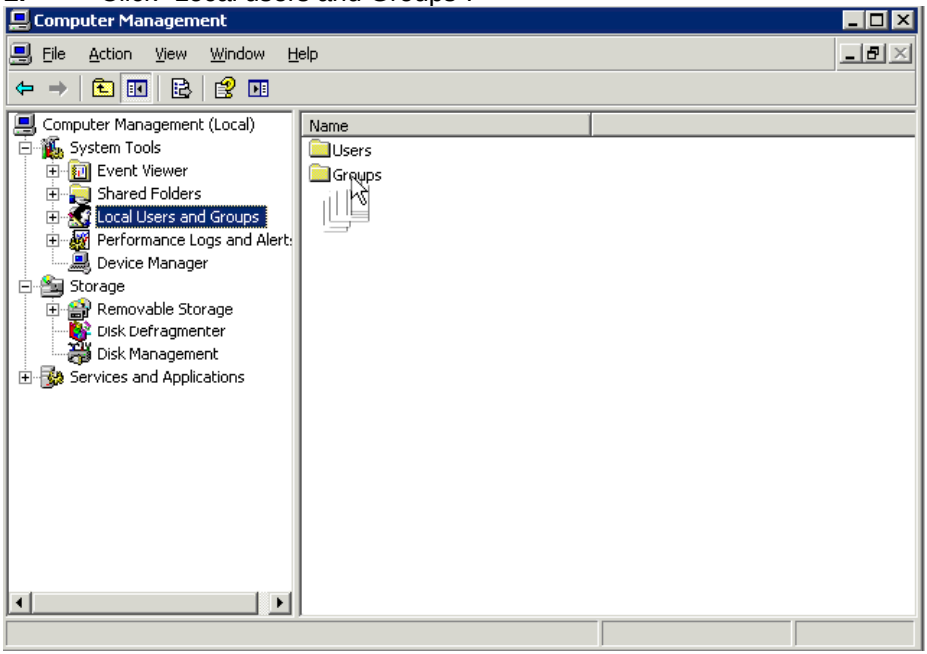
The following section details how to add users to HP groups..

Right click **“My Computer”.**

1. Click Manage.

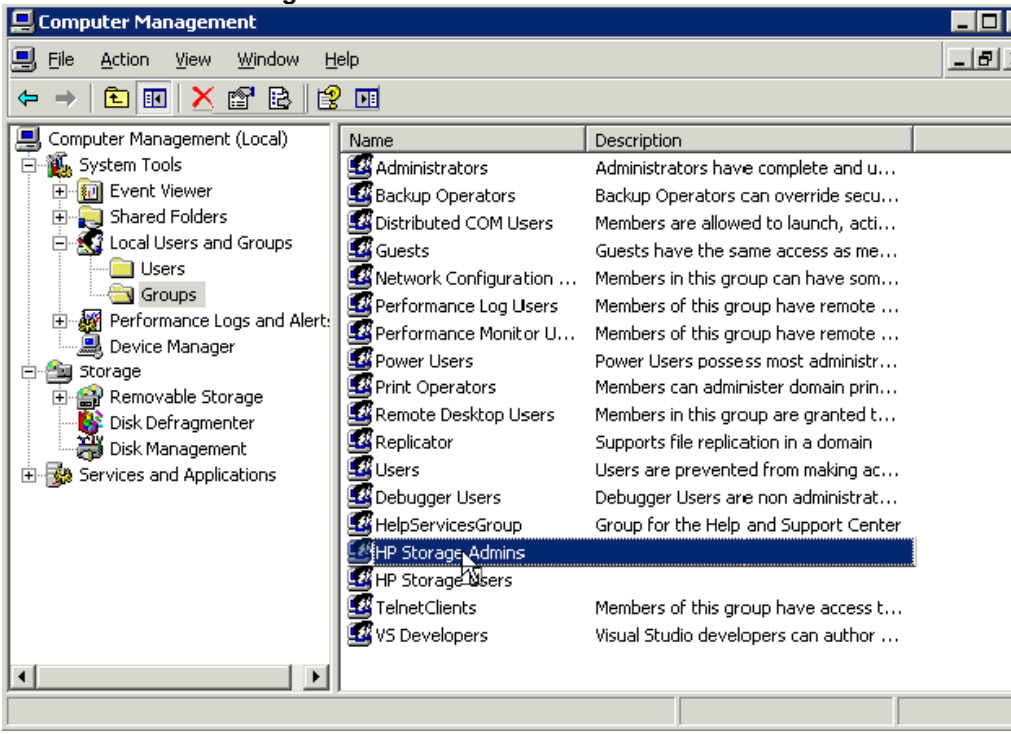


2. Click “Local users and Groups”.



3. Click **Groups.**

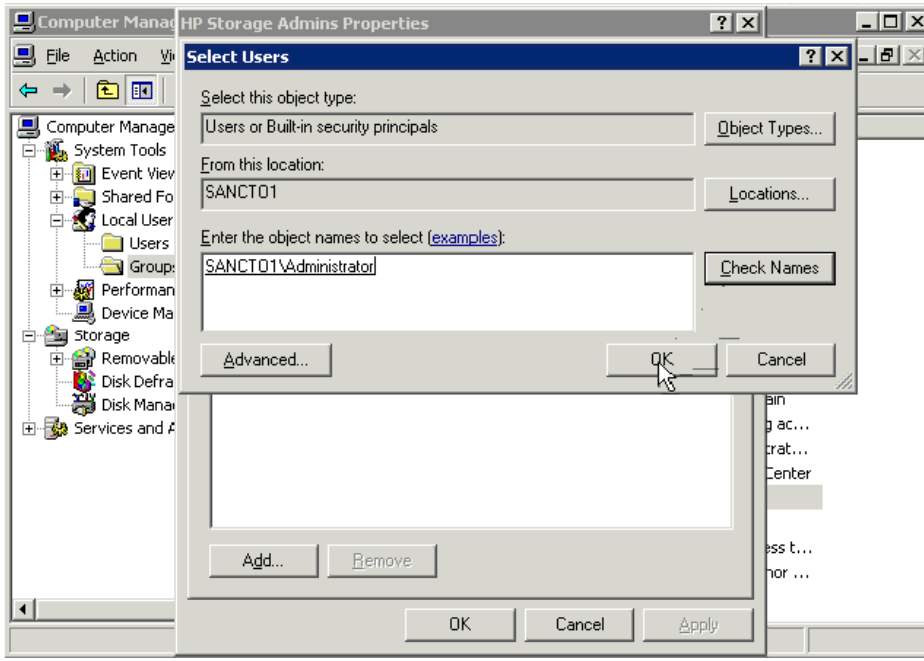
4. Double Click “**HP Storage Admins**”.



5. Click **Add.**

Enter the names to be added.

6. Click **OK**.



7. Click **OK.** This will return you to the Computer Management screen.

Double click HP Storage Users.

Follow the steps for adding the same user to the HP Storage Users group.

Troubleshooting HP EVA

Q: What is the minimum Command View version I should be using for EVA?

A: Command View 8.0.2

Q: What is the default user name password?

A: The user must be a valid user for the Command View. The default username/password is administrator/administrator.

Note: With Command View 8.x and 9.x, if you want to use a local user to login you have to use it like MACHINENAME\localuser

Q: How do I check if the user is a valid user for the provider?

A:

For Command View version 7.0 or below:

The user must be a valid local system user(domain user is not enough).

User has to be added to the provider using the cimuser utility.

Can choose a different password when adding using via 'cimuser' utility.

- **Note:** User may get removed from the provider when the provider service gets restarted.

Use the cimuser utility to list the users already added to the provider.

For Command View version 8.0 and above:

EVA provider users are valid Command View Users.

Command View users are valid Windows domain users belonging to HPStorageUsers or the HPStorageAdmins group.

Verify by logging into the Command View GUI using the same userid and password.

Q: SMI-S commands are failing with ACCESS DENIED errors. What do I need to check?

A:

1. Verify that the user is a valid user. You can verify that by logging into the Command View GUI with same user name and password.

2. Verify the user account is not locked out.

(Local users and Groups→ users→ <username>→Properties --

make sure check box 'Account is Locked out' is not checked.)

Q: What happened to the cimuser utility in Command View EVA 8 and above?

A: The cimuser utility used to manage users for the CIM Provider in previous versions (7.x and before) is no longer available in Command View 8. Only Command View users are valid users for SMI-S EVA. Command View users are normally Windows domain users.

Q: Why are we not getting performance data?

A: Requires Command View 8.0.2 or above to get the performance data.

Verify the following steps:

Performance data is not available if firmware is ‘6110’. This is due to a known issue where port WWN is zero. Solution is to upgrade to firmware version 6200

‘HP EVA Perf’ template must be selected from profiler for the device.

Check if the logs show ‘Duplicate host port address on EVA controller” exception when getting performance data. This is a known issue. There are two possible resolutions to the issue:

Upgrade the firmware to 6200 as this firmware has fix for the issue

Change the hardware connections such that the same ports of an array are not connected to same ports on switches with same domain name.

Make sure 'HP EVA Performance Data Collector' service is running.

Q: What performance metrics are available for EVA?

A: Perf metrics are available for these classes from provider v8.0.2; though we have implementation (only basic) we don’t claim support for performance provider part of EVA:

- - Storage System
- - Storage System controller
- - Volume
- - Front-end Port

Q: Where can I download latest Command View EVA?

A: Cannot be downloaded. Customers must contact their HP rep.

Q: Why do I see SNMP Traps in Profiler with messages of invalid namespace /root/pg_interop after Command View EVA was upgraded to v8?

A: /root/pg_interop is no longer a valid namespace. Change both cimom and vendor namespaces in mod.sys.smis.smis.xml to /interop

Q: Which service is the SMI-S provider in Command View EVA 8?

A: HP StorageWorks CIM Object Manager service is the SMI-S provider service

Q: How do I change the port for the SMI-S provider in Command View?

a. Stop the HP StorageWorks CIM Object Manager service (Services window)

b. Change the parameters *cxws.http.port* and *cxws.https.port* in the cxws.properties(C:\Program Files\Hewlett-Packard\SMI-S\CXWSCimom\config\cxws.properties) file.

Q: How do I enable/collect logging?

a. Set the Provider and CIMOM Log Level by executing the command, <InstalledPath>\Hewlettpackard\SMIS\CXWSCimom\bin\cscript Set_LogLevel.vbs <LogLevel>

The log levels are: ALL/DEBUG/ERROR/INFO/WARN/OFF

Eg: C:\Program Files\Hewlett-Packard\SMI-S\CXWSCimom\bin>cscriptSet_Log-Level.vbs ALL

b. Collect the Provider and CIMOM logs as a zip file by executing the command, <InstalledPath>\Hewlett-Packard\SMI-S\CXWSCimom\bin>cscript Collect-Logs.vbs.

c. Command View logs are located at, <InstalledPath>\Hewlett-Packard\Sanworks\Element Manager for StorageWorks HSV

Note: Make sure the debug logging is turned off after the logs are being collected. HP does not recommend turning on DEBUG logs except for diagnosis.

Configuring HP SMI-S EVA logging using Dynamic log level setting tool

This tool facilitates changing the log levels of both the CIMOM and HP SMI-S EVA Provider without the need to restart the service.

NOTE: The log levels are: ALL/DEBUG/ERROR/INFO/WARN/OFF

• The log levels are case sensitive. Ensure that you provide the desired log level in uppercase only.

• After you change the log level, it may take a few minutes for the changes to take effect.

To change the log level:

1. Open a command prompt window.

2. Set the path to the specified directory as in the following example:

Installed Path\Hewlettpackard\ SMIS\CXWSCimom\bin

3. Enter the Set_LogLevel command as displayed in the following example:

cscript Set_LogLevel.vbsloglevel

After you enter the CIMOM and HP SMI-S EVA Provider Set_LogLevel command, the log level is set to the desired log level. The following example message is displayed:

Log Level Set to: log level.

For example: if you enter

C:\Program Files\Hewlett-Packard\SMI-S\CXWSCimom\bin>cscriptSet_Log-

Level.vbs ALL. The output is displayed as:

Set_LogLevel.vbs ALL

Troubleshooting Using the CollectLogs tool

This tool facilitates archiving all log and configuration files required for debugging to a specified temporary folder.

To archive the files:

1. Open a command prompt window.

2. Set the path to the specified directory as in the following example:

Installed Path\Hewlettpackard\ SMIS\CXWSCimom\bin

3. Enter the CollectLogs command script as displayed in the following example:

cscript CollectLogs.vbsloglevel

After you enter the CIMOM and HP SMI-S EVA Provider CollectLogs command script, the following example message is displayed:

Information collected successfully Location: C:\Program Files\Hewlett-

Packard\SMI-S\Zip Folder Name.

For example: if you enter

C:\Program Files\Hewlett-Packard\SMI-S\CXWSCimom\bin>cscript Collect-

Logs.vbs. The output is displayed as:

Information collected successfully Location: C:\Program Files\Hewlett-

Packard\SMI -S\support_ d200896_t105335.zip

Note: Make sure the debug logging is turned off after the logs are being collected. HP does not recommend turning on DEBUG logs except for diagnosis.

Command View logs are located at,

C:\Program Files\Hewlett-Packard\Sanworks\Element Manager for StorageWorks HSV

Q: Provider is not discovering the EVAs after a fresh install or provider is not able to synch with the EVA after running for a while.

- Install the trust certificate between Command View and SMI Provider(see next topic for instructions)
- For Command View Version 8.0.1 or below, restart the server where the provider is running if it has not been restarted for more than 26 days. This is a known bug and it is fixed in Version 8.0.2.
- Make sure the provider is using the valid Command View EVA IP. If the Command View EVA Server IP address changed, it is not necessary that it gets updated for the SMI-S provider.

This can be verified by running the following command:

<InstalledPath>\Hewlett-Packard\SMI-S\EVAProvider\bin> discoverer.bat

```
Eg:
C:\Program Files\Hewlett-Packard\SMI-S\EVAProvider\bin> discoverer

==========================WELCOME TO THE DISCOVERER==============

Enter the SMIS host [default: http://localhost:5988] :
Enter the SMIS username :Administrator
Enter the SMIS password :

Connecting to EVA SMIS in http://localhost... Please wait....

_____________________________MENU_____________________________

1.Add a CV IP
2.Remove a CV IP
3.Get the list of CV IPs
0.Exit

Please enter your choice :3

_________CommandViews currently discovered by SMIS__________

172.192.18.204
```

If it is not found to the valid Command View EVA Server IP, add the correct IP using 'discoverer.bat' . Then remove the invalid IP.

- Refresh the smis provider cache using the command <InstalledPath>\Hewlett-Packard\SMI-S\CXWSCimom\bin> CLIRefreshTool.bat

The result will show if the refresh was successful or not.

- You can also check on the status of the periodic refresh of the cache using the command, <InstalledPath>\Hewlett-Packard\SMI-S\CXWSCimom\bin>GetArrayRefreshStatus.bat <Username> <Password>

Q: How do I install the trust certificate between provider and command view?

A:Please select the "Server Options" in the CV EVA GUI. (Top right side)

Please click on the "Other application trust relationships" option (check box).

Remove the existing certificate using "Uninstall Certificates" option.

Install the new certificate (HPSMISSSO.cert) using the "Install Certificate" option.You need to give the certificate location and the name (name can of your choice).

HPSMISSSO.cert certificate can be found at

Command View Version 8.0 or above

C:\Program Files\Hewlett-Packard\SMI-S\EVAProvider\config "

Q: Why cim commands fail with invalid namespace errors when using /root/eva?

A: Command View Version 8.0 or above

- Run SMISProvider\bin\registerEVAProvider.bat
- Restart the provider service.

Q: What files are needed to send a bug to HP?

A: Provider log files (refer to above question 'How do I enable logging?' for log location and settings)

- Model and firmware levels of EVAs being monitored

- Output of the following commands

Open a command prompt <SMIS install folder>\ CXWSCimom\bin and execute the following commands

cxmofd.bat -h http://localhost -l username:password -n interop cim_namespace

cxmofd.bat -h http://localhost -l username:password -n interop cim_objectManager

cxmofd.bat -h http://localhost -l username:password -n root/eva -i hpeva_storagesystem

cxmofd.bat -h http://localhost -l username:password -n root/eva -i hpeva_storagevolume

- Command View version info

- ***If it is an issue with performance, include the output of the following evaperf commands.***

- a. evaperf as
- b. evaperf pd
- c. evaperf vd
- d. evaperf hps

Note: evaperf.exe is located under folder 'Hewlett-Packard\EVA Performance Monitor'.

Note: HP support requests log files in ALL level; however, the logs may be overwritten, or unable to reproduce issue after resetting log level. Be sure to explain thoroughly in email to support.

Q: Unable to get data from the provider after the provider is upgraded from an older version to version 9.0(or above). Why?

A: The older version of the provider must be completely uninstalled before installing the newer version of the provider until HP supports provider upgrades. Otherwise there are chances that provider from previous install is still running and using the default ports.

To verify,

Services Panel → make sure that service with name 'HP StorageWorks SMI-S CIMServer' does not exist. If exists, stop the service and disable it. Version 9.0 provider installs with the service name 'HP StorageWorks CIM Object manager'.

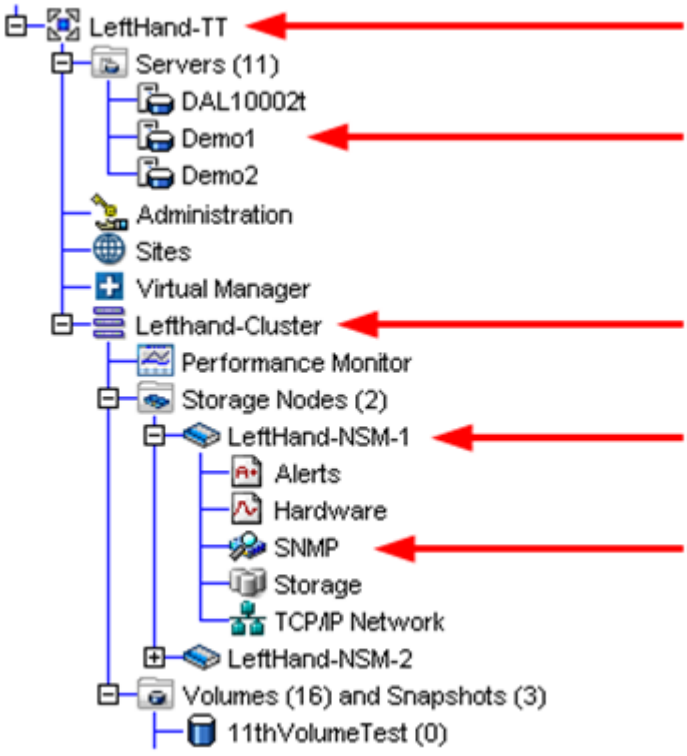
HP LeftHand

HP LeftHand Enabling SNMP

This section details enabling SNMP polling on the management nodes from the poller agent assigned to poll LeftHand devices. Once enabled, the SNMP data will appear within the LeftHand device console screen.

HP LeftHand CMC (Centralized Management Console) structure:

To begin you need to drill down in the cluster to locate a management node.

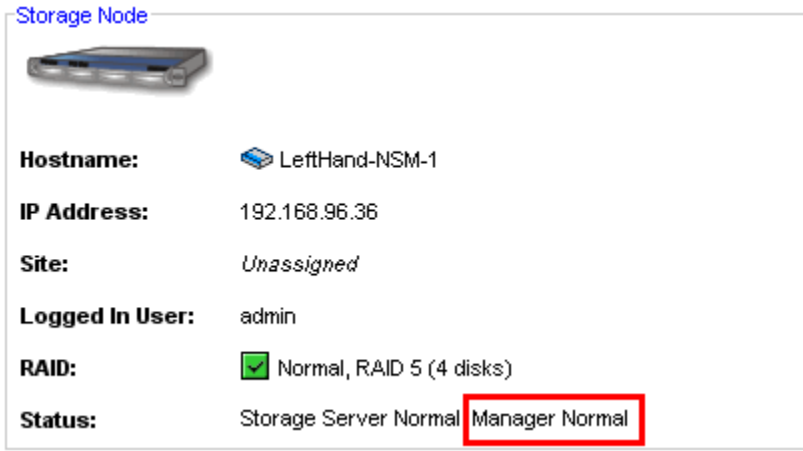


Finding a Management Node

To find a management node for a specific cluster

1. Click on the node and check the Status on the Details tab.

2. If the status reads Manager Normal then it is a management node.

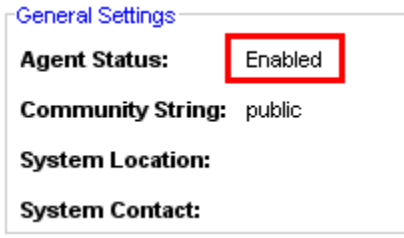


Enabling SNMP:

You need to have SNMP enabled and also allow the respective proxy agents to access the information. After adding permissions to one node you will then need to copy these permissions to the rest of the nodes.

To check if SNMP is enabled:

1. Click the SNMP icon below one of the nodes.
2. Check that Agent Status is enabled on the SNMP General tab.
3. If SNMP is not enabled, Edit SNMP Settings below will include how to enable it.



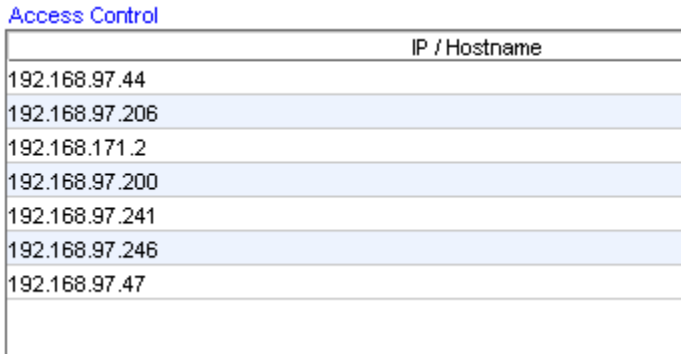
To Find Community String:

1. Click the SNMP icon below one of the nodes.
2. Check the Community String, if it is different than public make sure this is reflected within profiler.
3. If the Community String needs to be changed see **Edit SNMP Settings** below for steps.

Note: Community Strings are CASE sensitive and need to reflect their case sensitivity in Profiler as well.

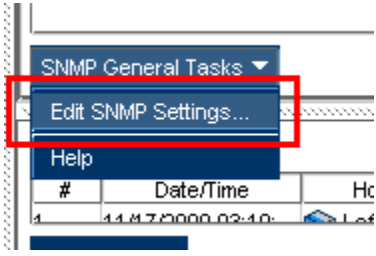
To check if proxy agent is in Access Control list:

Check the Access Control list and see if the proxy agent's IP address is in the list. If not, it will need to be added. To do so, see Edit SNMP Settings below.

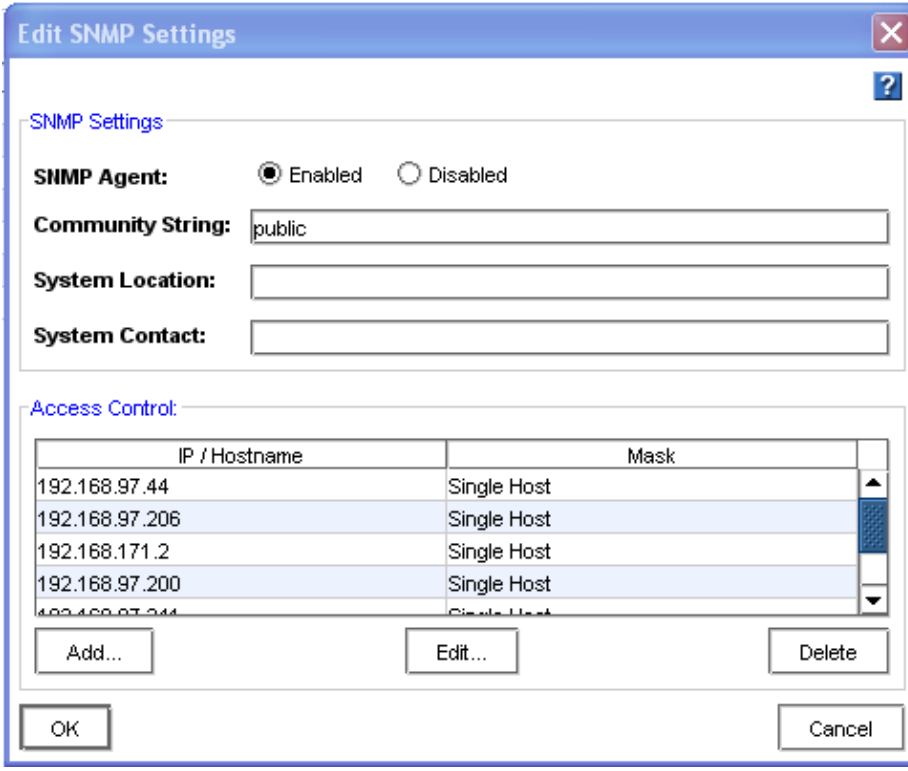


Edit SNMP Settings:

Near the bottom of the CMC screen there is a SNMP General Tasks drop down. From here click Edit SNMP Settings...

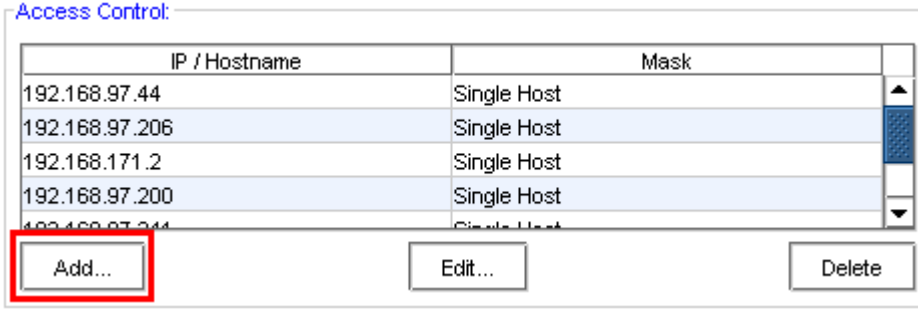


From this page you can set SNMP to enabled, change the Community String and add the proxy agent to the Access Control list.

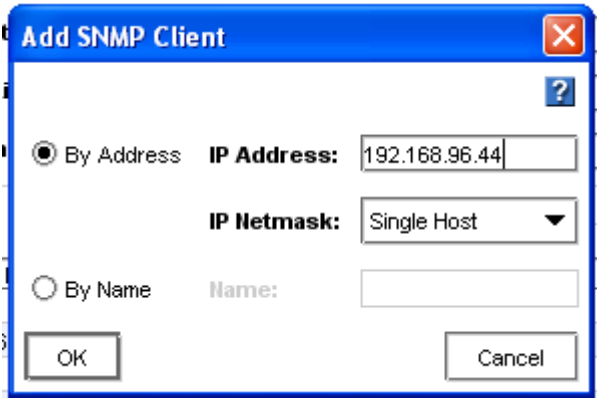


Add proxy agent IP to Access Control list:

From the Edit SNMP Settings page, click **Add**.

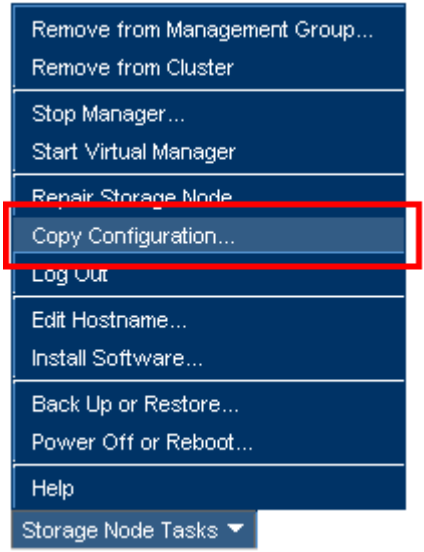


This will bring you to the Add SNMP Client page. From here, click the **By Address** radio button and add the IP address of the proxy agent and then click **OK**

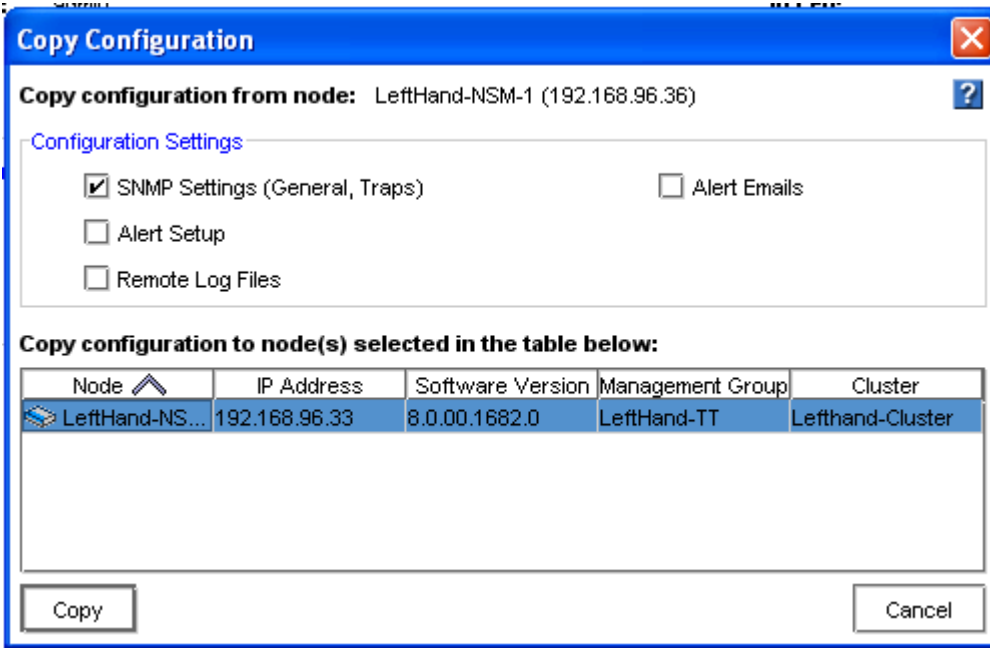


The proxy agent IP should now be in the Access Control list. The last step is to copy these SNMP settings to the rest of the nodes within the cluster.To do this return back to the node page.

From the Node page you can click on the Storage Node Tasks drop down at the bottom of the page and select Copy Configuration...



This will bring up the Copy Configuration box, and from here you can select the SNMP Settings and select the nodes you want to copy the configuration to by checking the checkbox for SNMP Settings (General, Traps) and by selecting the nodes you wish to copy the selected configuration to.



Once you click copy the configuration is copied to all the nodes selected. You should now see the proxy agent IP in each node's Access Control list.

1. Management Group
2. Servers
3. Cluster
4. Node
5. SNMP Settings

IBM DS Provider

The following section details installation links to versions of IBM providers. The correct IBM Provider to install is based on Model and Firmware.

For any **DS 6000, 8000 or ESS**, install the IBM Provider.

For any **DS 3k, 4k, or 5k array**, install the LSI Provider, covered in the "LSI Provider" section on page "233".

Compatibility Matrix: http://www-1.ibm.com/support/docview.wss?rs=1118&context=STC4NKB&dc=DB500&uid=ssg1S1002714&loc=en_US&cs=utf-8&lang=en

Note: The Bundle and LIC are firmware versions for the array. The compatibility matrix shows the minimum and maximum for the specific arrays and their providers.

IBM Provider Download:

http://www-947.ibm.com/support/entry/portal/Downloads/Hardware/System_Storage/Storage_software/Other_software_products/CIM_Agent_for_DS_Open_(API)/

IBM CIM Agent:

http://www-01.ibm.com/support/docview.wss?rs=1118&context=STC4NKB&dc=DB500&uid=ssg1S1003070&loc=en_US&cs=utf-8&lang=en

IBM Provider FAQ:

http://www-01.ibm.com/support/docview.wss?rs=1118&context=STC4NKB&dc=DB500&uid=ssg1S1003070&loc=en_US&cs=utf-8&lang=en

Install guides:

Search results link showing all documents for **DS Open API**

http://www-1.ibm.com/support/search.wss?rs=1118&tc=STC4NKB&dc=DA400+DB300+DA100+DA110+DA120+DB100+DA700+DA450+DA300&dtm

DS Open Application Programming Interface 5.4.1 and 5.4.2 Installation and Reference

http://www-01.ibm.com/support/docview.wss?uid=ssg1S7002719&aid=1

Troubleshooting IBM

The following section details FAQs for the IBM SMI-S Provider.

Q: Is IBM Shark supported?

A: Yes. Add it as an “IBM DS 6K/8K Series” device

Q: What is the default username/password for the IBM provider?

A: superuser / passw0rd

Q: What is service name for the IBM provider in windows?

A: “IBM System Storage CIM Agent for DS Open API x.y Pegasus Server”, where x.y is the version.

Q: Where are the logs located?

A: <install path>\logs

<install path>\pegasus\log

<install path>\pegasus\logs

Q: How do I add an array to the provider?

A: <install path>\bin\dscimcli mkdev <ip> -type <ds|ess> -user <username> -password <password>

Example: dscimcli mkdev 192.168.0.1 -type ds -user superuser -password passw0rd

NOTE: the user and password combination are that of the Control Station

Q: How do I remove an array from the provider?

A: <install path>\bin\dscimcli rmdev <ip> -type <ds|ess>

Example: dscimcli rmdev 192.168.0.1 -type ds

Q: I try to add an array, but it fails with error ‘Array is already added’?

A: The password for the Control Station user may be expired, which can be verified in the <install path>\pegasus\log\providerdebug.log. If expired, the password can be reset in the Control Station.

Q: Where can I find more usage details on the dscimcli command?

A: Follow the link above for ‘Reference Install guides’. There are install/ref guides for 5.2, 5.3, 5.4 versions of the provider

Q: What user/password do I use when configuring the array in Profiler (in the monkey wrench page)?

A: Use the default username/password (superuser/passw0rd).

Other user-ids/passwords can be created using the dscimcli command. You can list what users are configured by doing ‘lsuser’

Q: What username/password do I use when adding array to the provider?

A: The username/password used for the Control Station (similar to how there is username/password to Navisphere). The user should know this information

Q: In what release did the CIM Agent become embedded in the HMC (Hardware Management Console)?

A: Starting with Release 2.4 (Bundle 6.2.400.64) of the DS8000, the CIM agent was embedded into the HMC. Up to Release 4 (Bundle 62.0.175.0) by default, it comes disabled

Q: How does the embedded CIM Agent get Enabled?

A: In order to use the CIM agent, the customer must contact IBM support to have the CIM agent enabled.

Q: How does the embedded CIM Agent get configured?

A: The Customer must download the dscimcli tool and install it on a separate server, i.e. the TPC server or laptop, to configure the CIM agent. dscimcli is a small utility that runs on the same platforms that the proxy CIM agent runs on, but does not consume a lot of CPU or memory, so it should be able to run on any reasonable server or laptop. You can download the dscimcli tool at the download site for the version of CIM agent that is running on the HMC. Please refer to the install documentation for more details.

Install Document Link: http://www-01.ibm.com/support/docview.wss?uid=ssg1S7002719&aid=1

Q: How do I enable the embedded CIM agent on the HMC?

A: For releases prior to DS8000 release 4.1, the CIM agent is NOT automatically enabled. You must enable the CIM agent on the HMC before you can use it. For DS8000 release 4.1 and later, the CIM agent is enabled by default. You do not have to enable the CIM agent unless it has been disabled.

Note: Enabling DS8000 CIM Agent on DS8000 bundles 6.2.400.64, 6.2.400.66, 6.2.400.76, and 6.2.410.30 requires assistance from IBM Technical Support.

Perform the following steps to enable the HMC CIM agent:

1. From the HMC Welcome page, click **HMC Management**. The HMC Management window is displayed.

2. Click Start/Stop CIM Agent. The HMC CIM Agent window is displayed with the current state of the CIM agent.

3. Select Start CIM Agent and click Apply. The CIM agent is started and the state is updated.

Q: How do I configure the embedded CIM agent for HMC?

A: For DS8000 release 4.0 and earlier, the CIM agent administrator and storage administrator are required to create and maintain user passwords for both the CIM agent and the DS8000 management applications. For DS8000 release 4.1 and later, the embedded CIM agent does not require configuration changes to manage DS8000 devices.

The DS8000 device user names and passwords are used to authenticate CIM client requests. The DS8000 administrator must create user names and passwords that CIM clients can use to attach to the CIM agent. Each user that is created must be in the administrator group. Users that are created in any group other than the administrator group cannot function with DS8000 release 4.1 and 4.2 CIM agents. The DS8000 administrator can use the DSCLI or the HMC console GUI to create the user names and passwords

Q: How do I verify the CIM agent connection to the HMC outside of Profiler?

A: You must verify that the CIM agent software connects to the storage unit that you identified during configuration by issuing the following command:

dscimcli -s https://<hmc_ip>:6989 -u <DS8000user> -p <DS8000password> lsdev -1

<hmc ip> is the IP address of the HMC, <DS8000user> is the user name that is used to log into the DS8000 Storage Manager, and <DS8000password> is the password that is used to log into the DS8000 Storage Manager.

Q: How do I setup Profiler to connect to the embedded HMC CIM agent?

A: Profiler should be configured with the same ports and credentials that were used to verify the HMC connection with the dscimcli.

HTTP Port: 6988 - This is the typical default port>

HTTPS Port: 6989 - This is the typical default port>

Provider IP: Use the HMC IP Address

Username – An administrator user, preferably the one used to verify the connection to the CIM agent

Password – The corresponding password to the user with administrator privileges used to connect to the CIM agent.

Identifier – Example: ibm.2107-75z9271 - This can be found in the Profiler SMI-S logs or by using the “Confirm Provider” button in the Array configuration page of Profiler.

IBM SVC Provider

The IBM SAN Volume Controller (SVC) SMI provider is embedded in each cluster.

Note: Older versions of SVC have another CIMOM embedded on the Management Console which is named as the proxy provider. IBM recommends not using this proxy CIMOM due to various performance considerations. Profiler must use the CIMOM on the cluster.

SVC (SAN Volume Controller) CIM Agent Download:
http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/supportresources?brandind=5000033&familyind=5329743&taskind=2

SVC CIM Agent Support Matrix:
http://www-1.ibm.com/support/docview.wss?rs=591&uid=ssg1S1002888#_SVC_and_SVC

CIM Agent documentation for various versions is available at:

ftp://ftp.software.ibm.com/storage/san/sanvc/V<x.x.x>/pubs/English/English_CIM_Agt_Dev_Ref.pdf

substitute <x.x.x> with the svc version. Eg: 4.2.0

More documentation is available at
http://publib.boulder.ibm.com/infocenter/svcic/v3r1m0/index.jsp?topic=/com.ibm.storage.svc.learning/learning_tutorials.html

Troubleshooting IBM SVC Provider

Q: What is the minimum version of the provider supported?

A: Minimum version supported is 4.3.1

Q: What is the default login and password the cim agent on the cluster?

A: Login is either administrator or superuser

Password is either passw0rd or l0destone

Q: What is the default port used by the cim agent?

A: By default the install uses HTTPS. If the user doesn't remember the ports/protocol used at install, the install directory contains a config file which will tell you: **svcconsole\cimom\pegasus\cimserver_current.conf.**

Q: Is it possible to upgrade the provider part alone?

A: No. The CIMOM is a core part of the SVC Console so you have to upgrade it as a part of your Console upgrade. The supported upgrade path is that you can run an SVC Console one rev up of the cluster code for migration purposes only. So you can upgrade the SVC Console to one rev up in order to upgrade the cluster, but IBM doesn't support long term management of mismatched SVC Console to Cluster versions.

SVC upgrade for cluster and console is a customer capable task; however, they should contact their IBM support representative to make sure they won't hit any of the known issues.

Q: For SVC 4.3.1 or above, provider exists on the cluster as well as on the host. Which one do I use?

A: From release 4.3.1 and above, there are multiple CIMOMs available; a) embedded CIMOMs in each cluster b) CIMOM on the management console (on the host where the SAN Volume Controller Console is running).

Use the CIMOM on the cluster. There are chances that the use of CIMOM on the management console slows down the SVC GUI operations. CIMOM on the cluster gives better performance than the other since it is embedded in the cluster itself.

Q: How do I find the IP for cluster?

Answer:

a. From the SVC GUI.

b. From TestProvider utility or from Confirm Provider in the Profiler GUI config page(only from Profiler version 4.9.1 or greater)

c. Connect to the CIMOM on the management Console .

d. Enumerate CIM_ComputerSystem class. IP of the cluster is part of the identifier for the cluster instance.

Q: How do I monitor multiple clusters?

A: Each cluster has to be configured in profiler as a SVC device with the correct CIMOM IP and identifier.

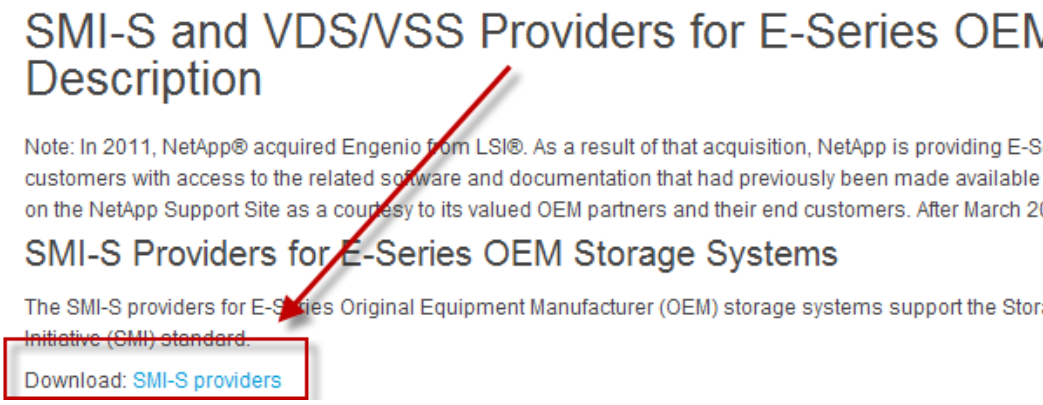
LSI Provider

As of June 2012, NetAPP (formerly LSI) released a new provider. We recommend using the new provider.

The download links are located on the NetApp support site. You will need to create an account to access the download link.

New Provider (Eagle 5) downloads are located here:
http://support.netapp.com/apbu/oemcp/protcd/

After logging in to the site, click the SMI-S Providers download link.

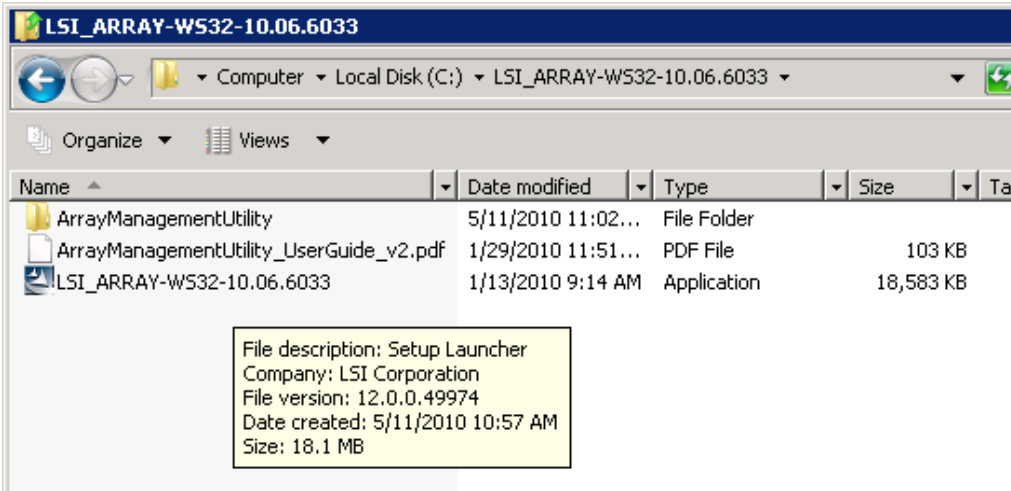

SMI-S and VDS/VSS Providers for E-Series OEM
Description
Note: In 2011, NetApp® acquired Engenio from LSI®. As a result of that acquisition, NetApp is providing E-S
customers with access to the related software and documentation that had previously been made available
on the NetApp Support Site as a courtesy to its valued OEM partners and their end customers. After March 20
SMI-S Providers for E-Series OEM Storage Systems
The SMI-S providers for E-Series Original Equipment Manufacturer (OEM) storage systems support the Stora
Initiative (SMI) standard.
Download: SMI-S providers

New Provider (Eagle 2)

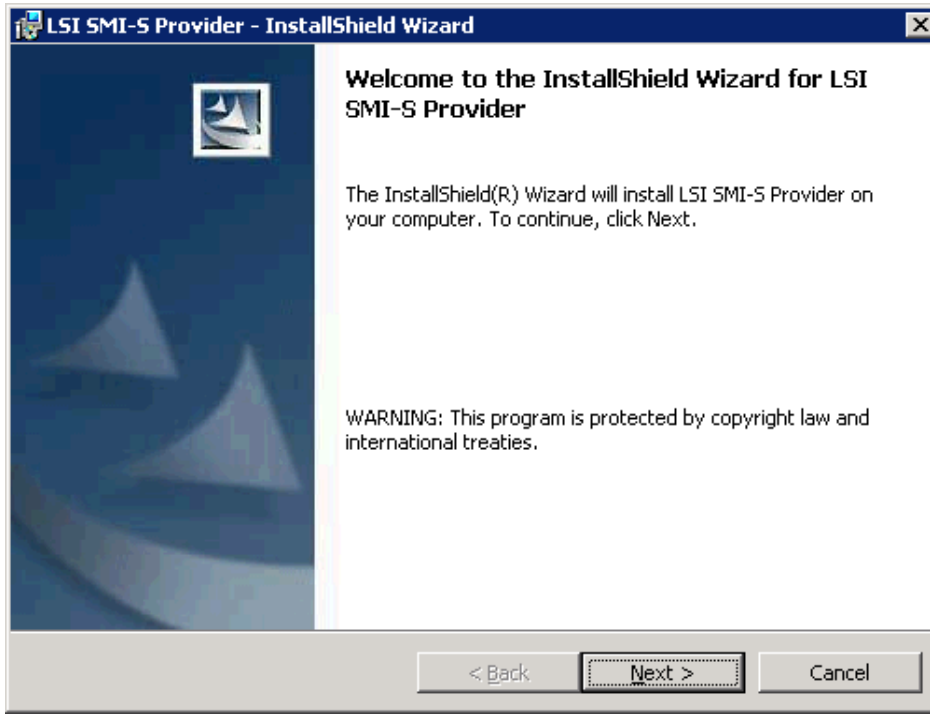
The following section details the steps for installing LSI on a windows server for the Eagle 2 Legacy version.

Installation for Windows

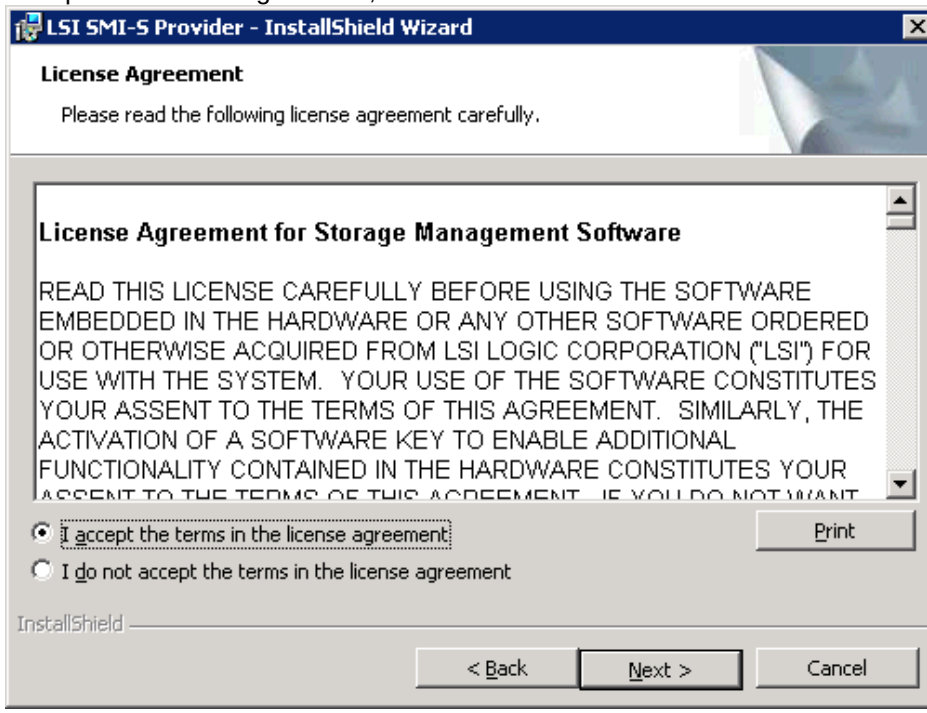
1. Double click the installer.



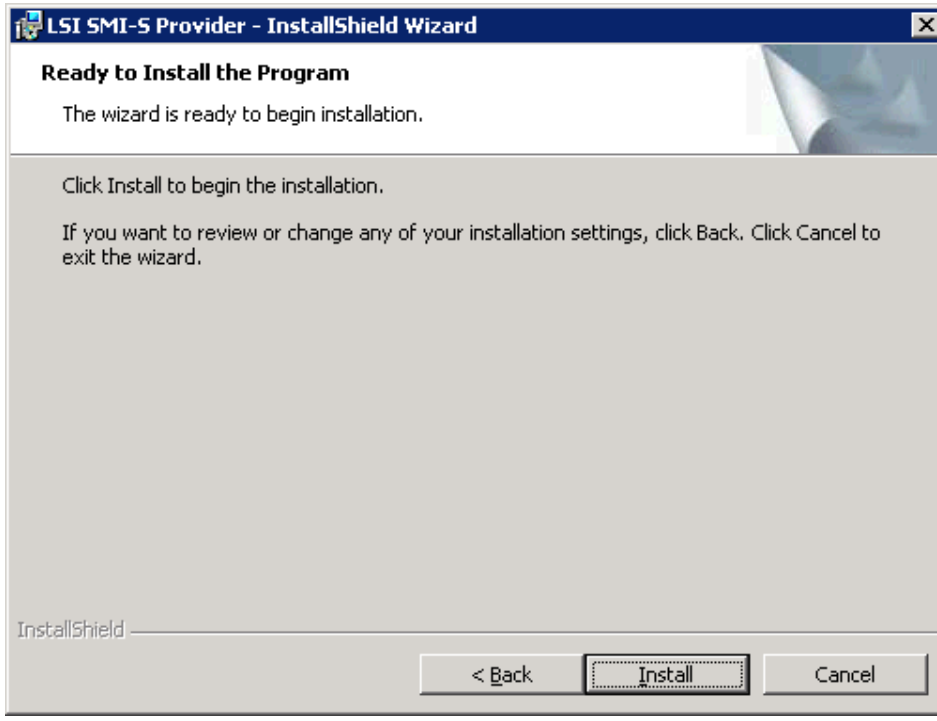
2. Click **Next** at the “Introduction” screen.


LSI SMI-S Provider - InstallShield Wizard
Welcome to the InstallShield Wizard for LSI SMI-S Provider
The InstallShield(R) Wizard will install LSI SMI-S Provider on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

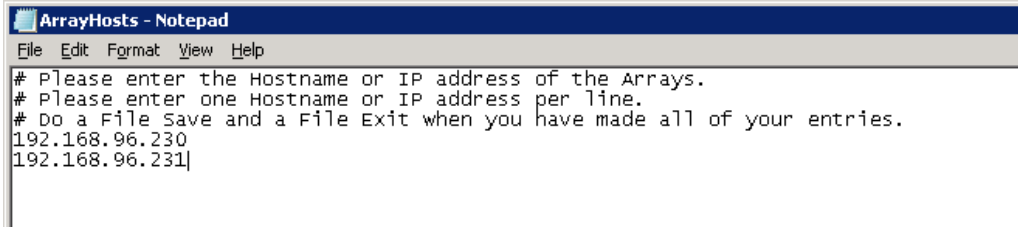
3. Accept the License Agreement, Click **Next**.


LSI SMI-S Provider - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
License Agreement for Storage Management Software
READ THIS LICENSE CAREFULLY BEFORE USING THE SOFTWARE EMBEDDED IN THE HARDWARE OR ANY OTHER SOFTWARE ORDERED OR OTHERWISE ACQUIRED FROM LSI LOGIC CORPORATION ("LSI") FOR USE WITH THE SYSTEM. YOUR USE OF THE SOFTWARE CONSTITUTES YOUR ASSENT TO THE TERMS OF THIS AGREEMENT. SIMILARLY, THE ACTIVATION OF A SOFTWARE KEY TO ENABLE ADDITIONAL FUNCTIONALITY CONTAINED IN THE HARDWARE CONSTITUTES YOUR
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

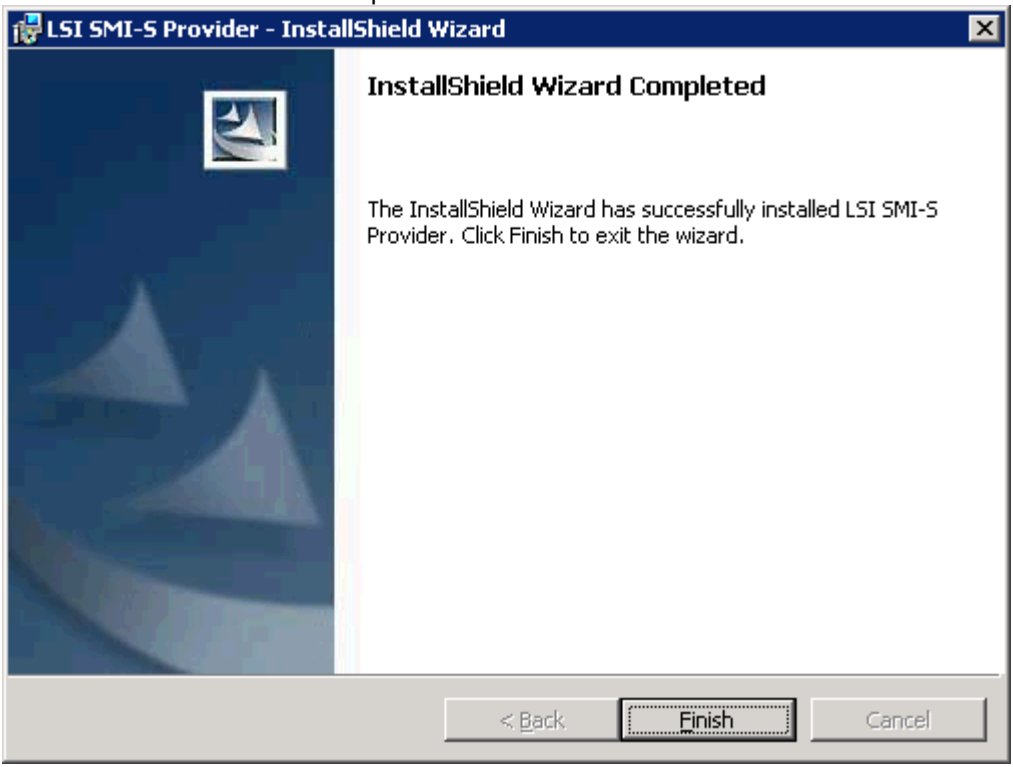
4. Click **Install.**


LSI SMI-S Provider - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

Add the IP addresses for the Array Controllers. Save and close Notepad.


ArrayHosts - Notepad
File Edit Format View Help
Please enter the Hostname or IP address of the Arrays.
Please enter one Hostname or IP address per line.
Do a File Save and a File Exit when you have made all of your entries.
192.168.96.230
192.168.96.231

Click **Finish** at the “Install Complete” screen.


LSI SMI-S Provider - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed LSI SMI-S Provider. Click Finish to exit the wizard.
< Back
Finish
Cancel

Installation for Linux

The following section details the installation steps on a Linux server.

1. Untar the lsi_array_xx.xx.xx.xx.tar file.

```
[root@localhost ~]# tar -xvf lsi_array-10.06.GG.33-1.rhel4.i386.rp
ArrayManagementUtility
ArrayManagementUtility_UserGuide_v2.pdf
lsi_array-10.06.GG.33-1.rhel4.i386.rpm
[root@localhost ~]# _
```

2. Execute rpm -i lsi_array_xx.xx.xx.xx.rpm.

```
[root@localhost provider]# rpm -i lsi_array-10.06.GG.33-1.rhel4.
Creating log directory.
Creating conf files.
Setting the OpenPegasus version
Checking the OpenPegasus version
Installing OpenPegasus 2.8.0. This may take a few minutes.
```

Adding A SAN

These following steps are taken for the arrays added during installation.

Installation on Windows

1. Run the ArrayManagementUtility.exe that came with the SMI-S installation file.

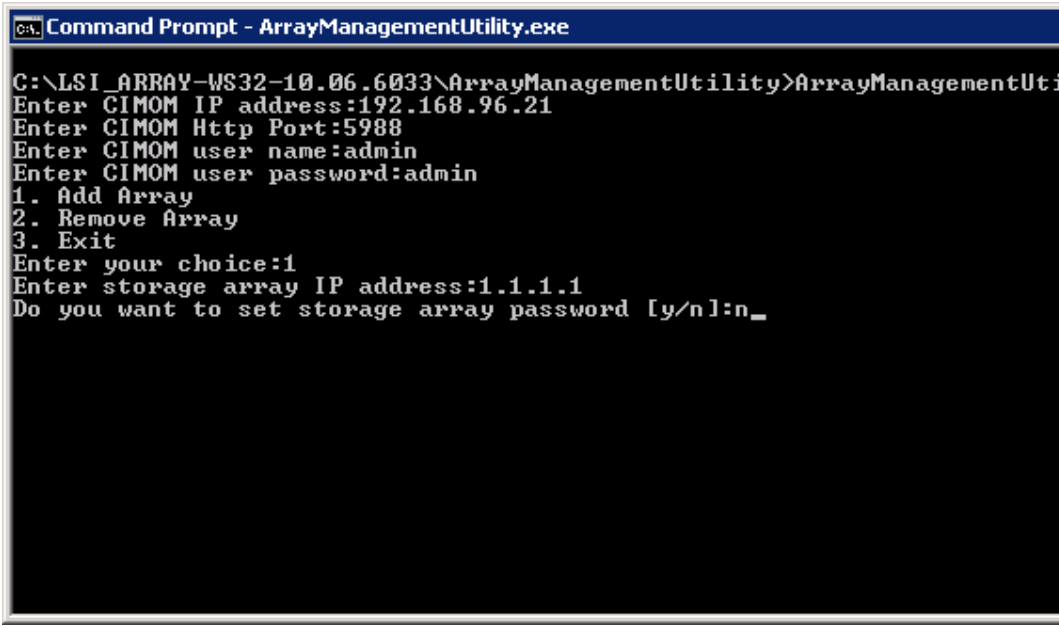
2. Use the IP where the SMI-S provider is installed.

3. Use the defaults for the CIMOM Username, Password, and Port.

4. Type 1 for Add Array.

5. Type the array IP or DNS name.

6. Type ***n*** to not set the storage array password.



Adding A SAN

Installation on Linux

1. Edit the /opt/lsi/sbma/data/ArrayHosts.txt file.

2. Enter the IP address of each array, one per line.

3. Stop the cimserver with `/opt/lsi/pegasus/bin/cimserver-s`

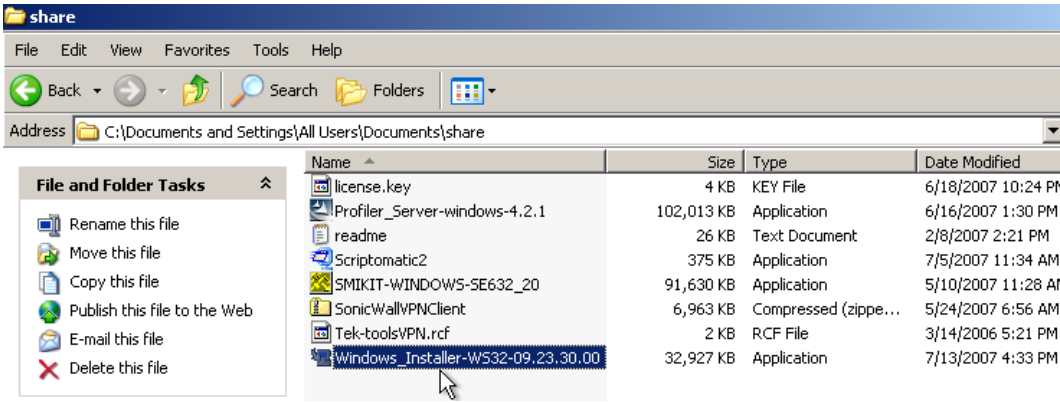
4. Start the cimserver with `/opt/lsi/pegasus/bin/cimserver start`

Legacy Provider (Pre-Eagle 2)

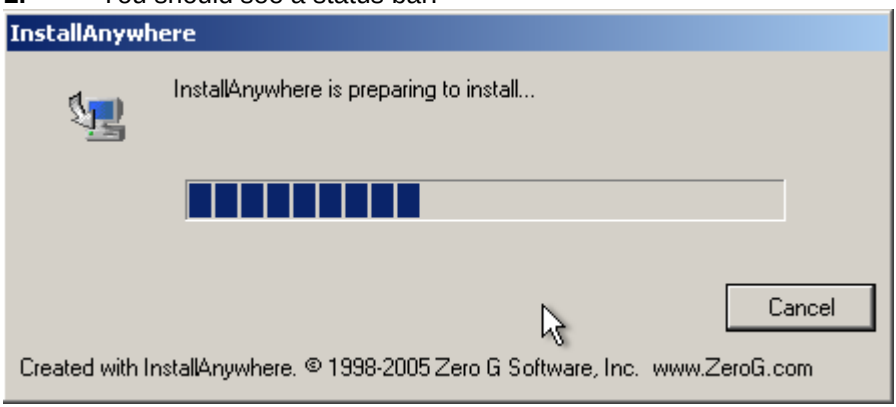
The following section details the installation on windows devices for pre-eagle 2 providers.

Installation on Windows

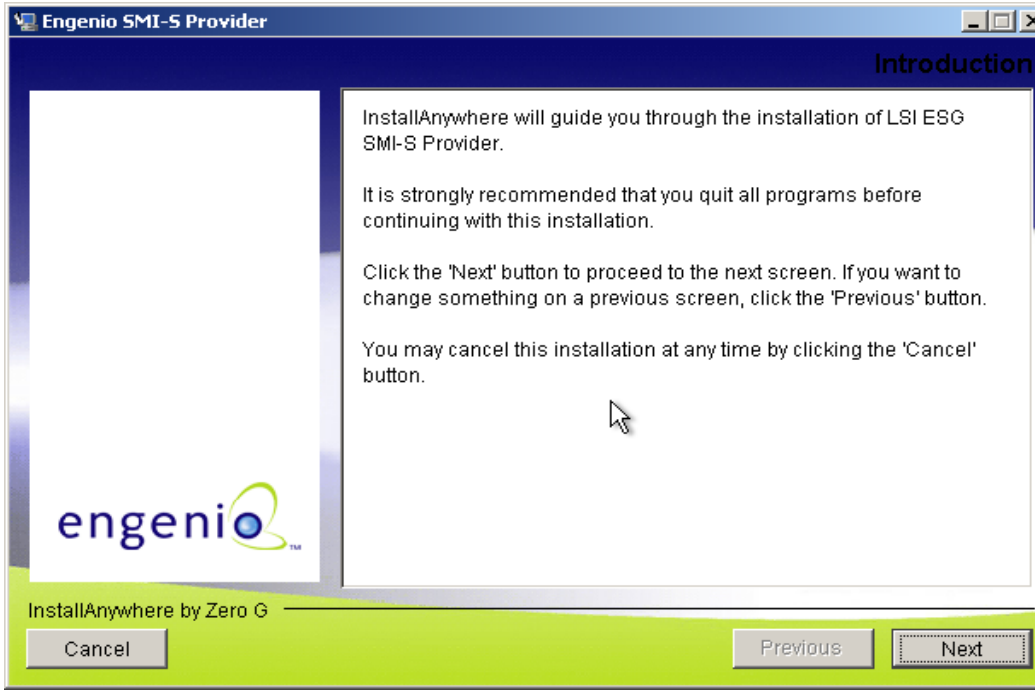
1. Double click the installer.


share
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\All Users\Documents\share
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Name Size Type Date Modified
license.key 4 KB KEY File 6/18/2007 10:24 PM
Profiler_Server-windows-4.2.1 102,013 KB Application 6/16/2007 1:30 PM
readme 26 KB Text Document 2/8/2007 2:21 PM
Scriptomatic2 375 KB Application 7/5/2007 11:34 AM
SMIKIT-WINDOWS-SE632_20 91,630 KB Application 5/10/2007 11:28 AM
SonicWallVPNClient 6,963 KB Compressed (zippe... 5/24/2007 6:56 AM
Tek-toolsVPN.rcf 2 KB RCF File 3/14/2006 5:21 PM
Windows_Installer-WS32-09.23.30.00 32,927 KB Application 7/13/2007 4:33 PM

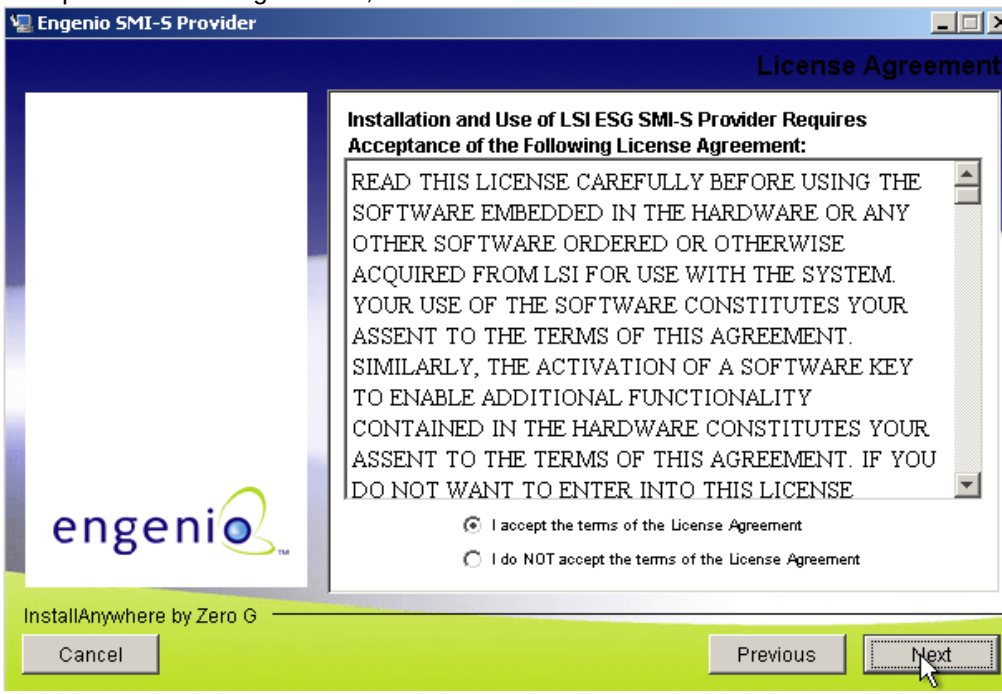
2. You should see a status bar.


InstallAnywhere
InstallAnywhere is preparing to install...
Cancel
Created with InstallAnywhere. © 1998-2005 Zero G Software, Inc. www.ZeroG.com

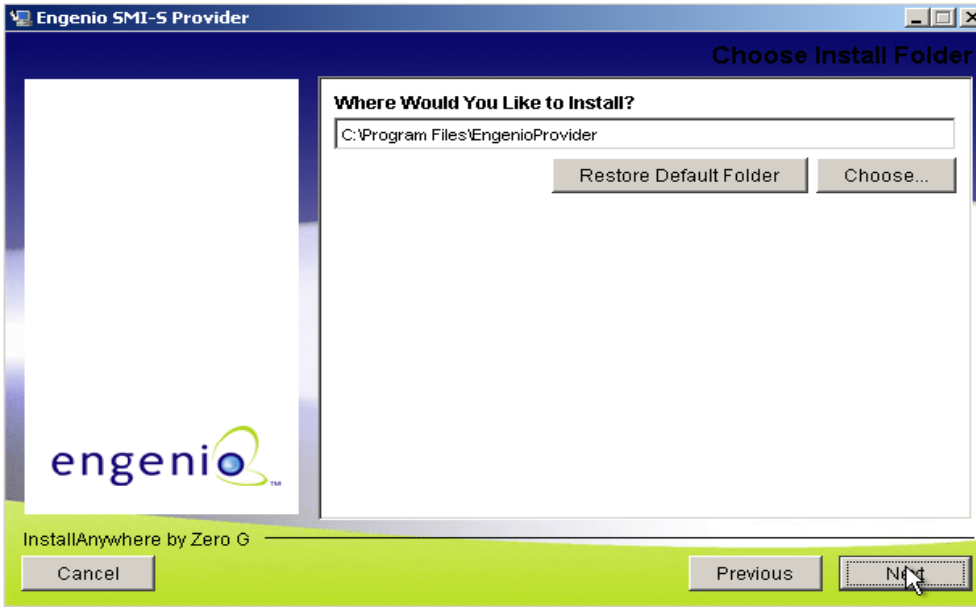
3. Click **Next** at the “Introduction” screen.


Engenio SMI-S Provider
Introduction
InstallAnywhere will guide you through the installation of LSI ESG SMI-S Provider.
It is strongly recommended that you quit all programs before continuing with this installation.
Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.
You may cancel this installation at any time by clicking the 'Cancel' button.
engenio
InstallAnywhere by Zero G
Cancel
Previous
Next

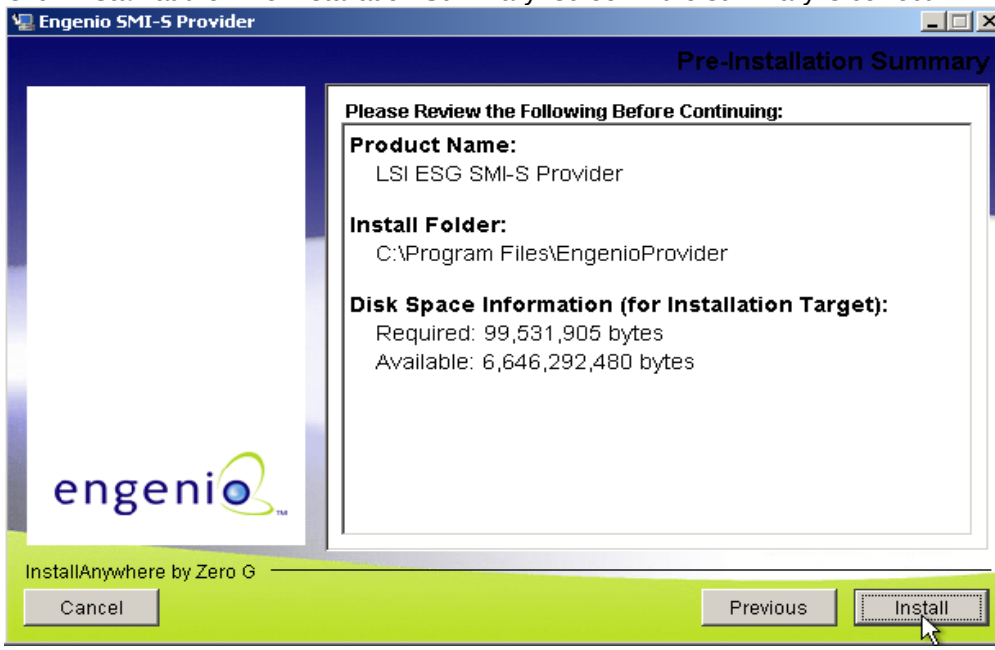
Accept the License Agreement, Click **Next.**


Engenio SMI-S Provider
License Agreement
Installation and Use of LSI ESG SMI-S Provider Requires Acceptance of the Following License Agreement:
READ THIS LICENSE CAREFULLY BEFORE USING THE SOFTWARE EMBEDDED IN THE HARDWARE OR ANY OTHER SOFTWARE ORDERED OR OTHERWISE ACQUIRED FROM LSI FOR USE WITH THE SYSTEM. YOUR USE OF THE SOFTWARE CONSTITUTES YOUR ASSENT TO THE TERMS OF THIS AGREEMENT. SIMILARLY, THE ACTIVATION OF A SOFTWARE KEY TO ENABLE ADDITIONAL FUNCTIONALITY CONTAINED IN THE HARDWARE CONSTITUTES YOUR ASSENT TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT WANT TO ENTER INTO THIS LICENSE
I accept the terms of the License Agreement
I do NOT accept the terms of the License Agreement
engenio
InstallAnywhere by Zero G
Cancel
Previous
Next

Choose the Install location, Click **Next.**



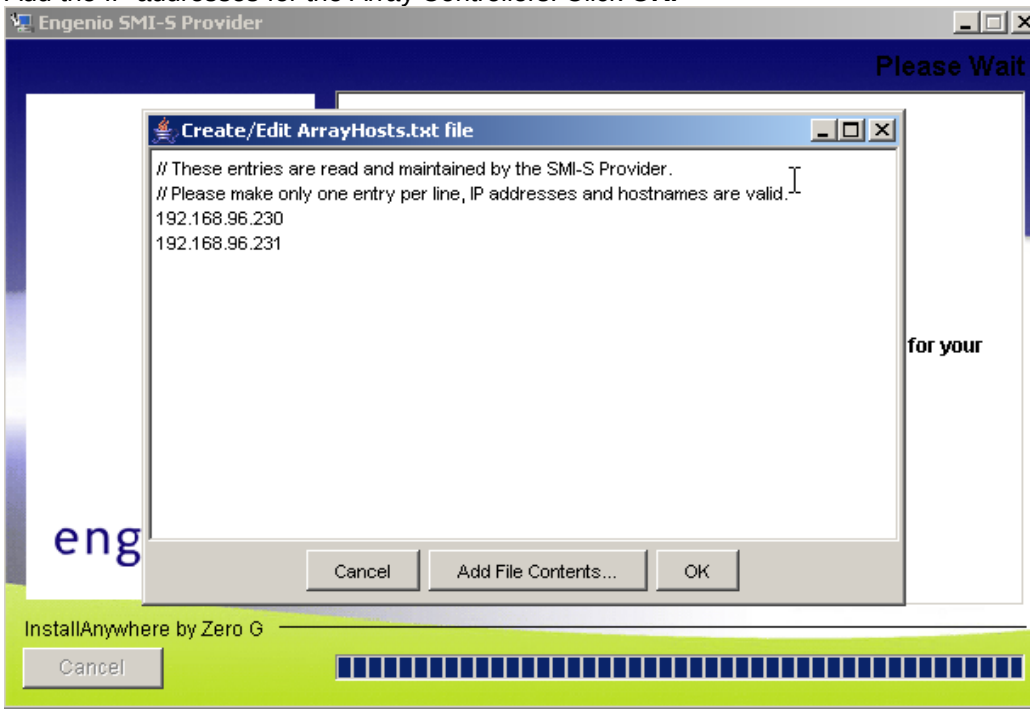
Click **Install** at the “Pre-Installation Summary” screen if the summary is correct.



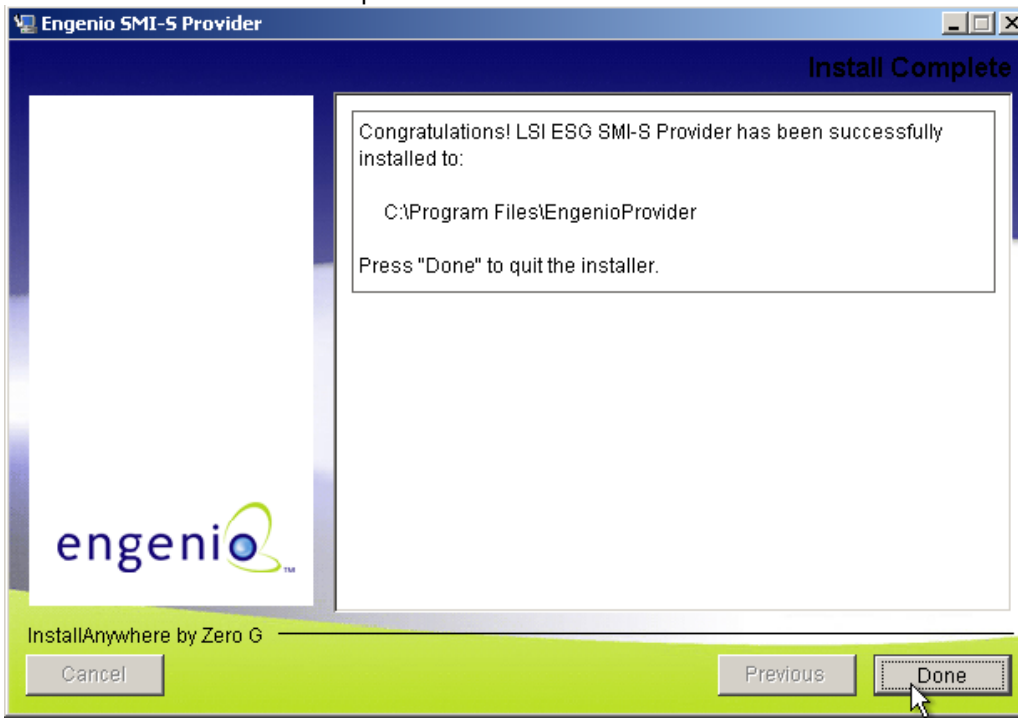
You should see the following screenshot:

Engenio SMI-S Provider
Installing LSI ESG SMI-S Provider
engenio
SMI-S Provider
engenio
Enable. Enhance. Empower.
Installing... Java Runtime Environment
InstallAnywhere by Zero G
Cancel

Add the IP addresses for the Array Controllers. Click **OK.**



Click **Done** at the “Install Complete” screen.



Installation on Linux

1. Untar the Linux_Installer_xx.xx.xx.xx.tar file.

```
[root@red-box LSI]# tar -xvf Linux_Installer_09.23.G0.00.tar
EngenioProvider-09.23.G0.00-0.i386.rpm
install
deinstall
[root@red-box LSI]# ls
deinstall                              install
EngenioProvider-09.23.G0.00-0.i386.rpm  Linux_Installer_09.23.G0.00.tar
```

2. Execute the install executable.

```
[root@red-box LSI]# ./install
Preparing packages for installation...
EngenioProvider-09.23.G0.00-0
EngenioProvider has been successfully installed on this computer.
The install location is /usr/engenio.

To start/stop EngenioProvider, issue the commands
'/etc/init.d/cimomd {start|stop|status|restart}'

It is recommended that EngenioProvider is only started/stopped through the
above command.
Note that starting EngenioProvider will also register and advertise its se
 using SLP.

EngenioProvider is now starting for the first time.
Starting the SMI-S Provider
```

Adding A SAN

The following section details the installation steps for adding SANs from windows and linux devices.

Windows

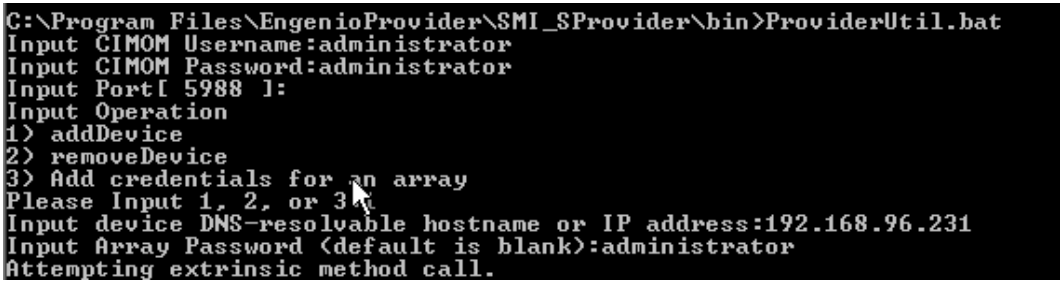
1. Run the <install directory>\SMI_SProvider\bin\ProviderUtil.bat script.

2. Use the defaults for the CIMOM Username, Password, and Port.

3. Type 1 for addDevice.

4. Type the array IP or DNS name.

5. Type the Array Password.



Linux

1. Run the /usr/engenio/SMI_SProvider/bin/ProviderUtil script.

2. Type the default username, password and Port.

Note: username - must be a valid user on the local system.

3. Type add for adding a device.

4. Type the IP or DNS name.

5. Type the array password.

```
[root@red-box bin]# ls
ConcreteVolumes.txt  portInfo.properties          ProviderUtil.bat
launch               providerStore                slp.properties
methodmappings.txt   providerTraceLog.properties
myKeyStoreFile       ProviderUtil
[root@red-box bin]# ./ProviderUtil
CIMOM username: \c
administrator
CIMOM Password: \c

Input CIMOM Port [5988]: \c

Input operation:
'add' for AddDevice,
'rem' for RemoveDevice: \c
add
Input IP or hostname for array: \c
192.168.96.230
Input Array password: \c

Attempting extrinsic method call.
The extrinsic call succeeded.
```

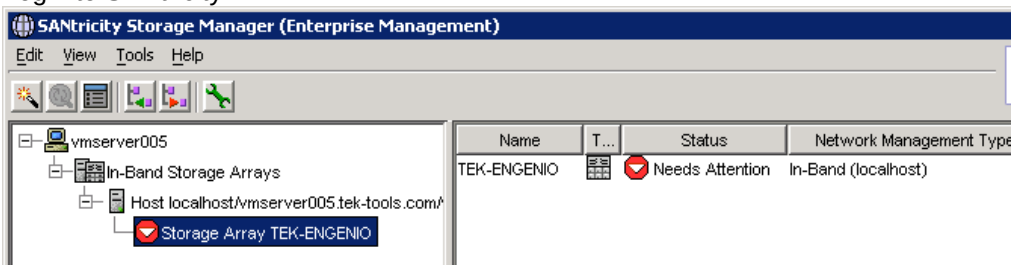
Obtaining Array Identifier

CIMWorkshop

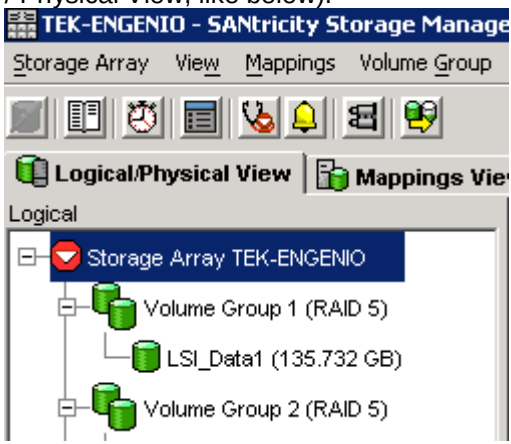
The LSI Provider has CIMWorkshop enabled, located:
C:\Program Files\EngenioProvider\wbemservices (by default).
Refer to Tools > CIMWorkshop for instructions on how to obtain the Array Identifier in CIMWorkshop.

SANtricity Storage Manager

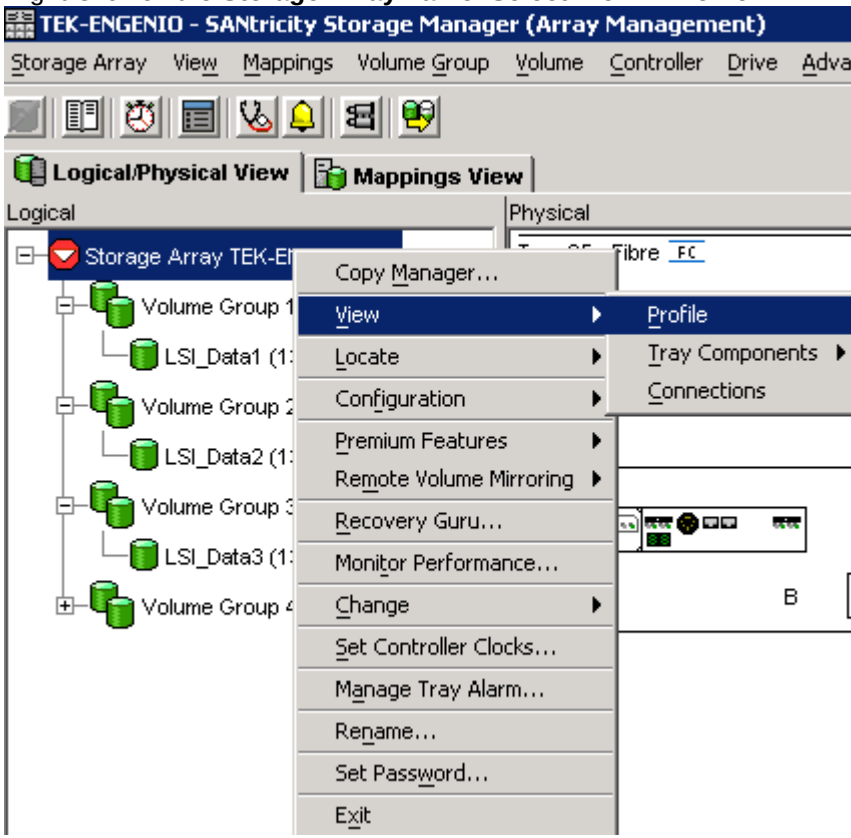
1. Log into SANtricity.



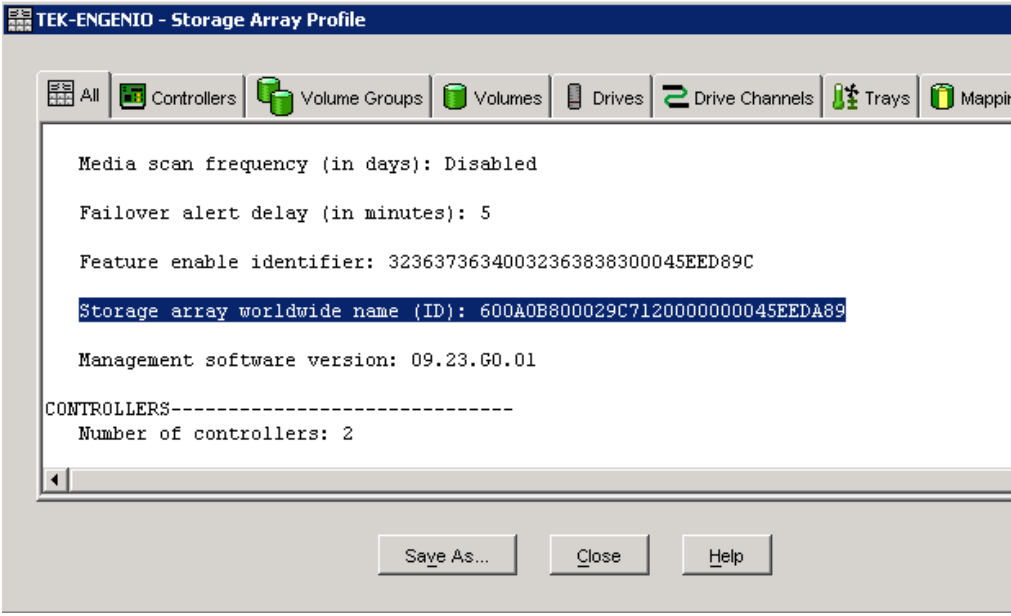
2. Double click on the **Storage Array name** (You should be taken to the Logical / Physical View, like below).



3. Right Click on the **Storage Array name. Select View > Profile**.

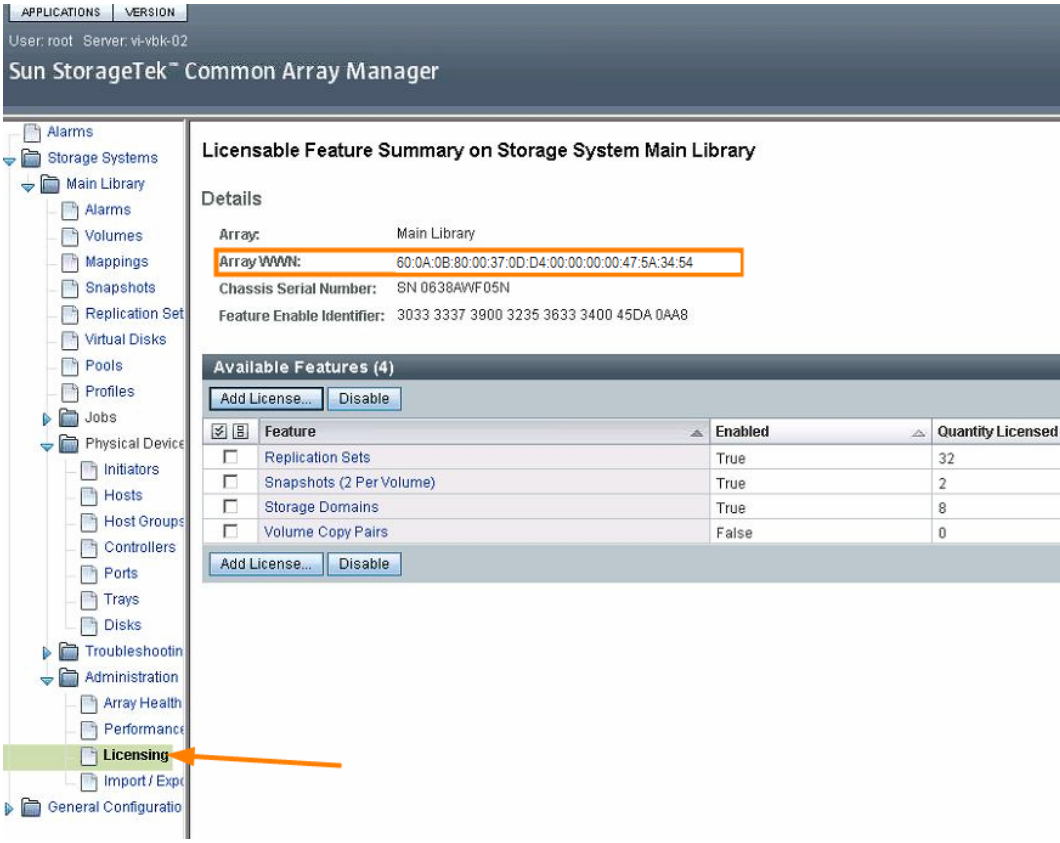


4. Scroll down to Storage array worldwide name (ID) under Summary for All tab.

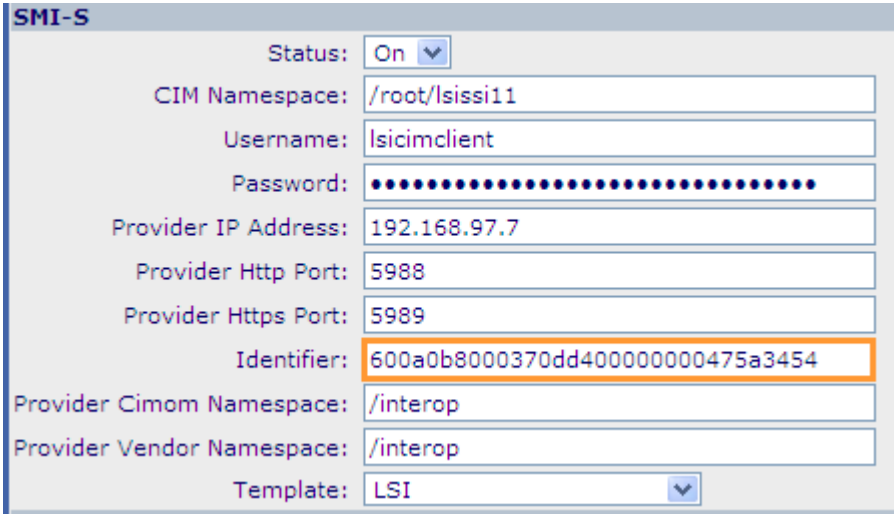


Common Array Manager

1. Login to Common Array Manager and click on the Administration → Licensing section and Note down the Array WWN as shown below



2. Remove the colons for providing the identifier within Profiler as shown below



Troubleshooting LSI New Provider Eagle 2

Q: What is the default username/password?

A: admin/admin

Q: What is the default namespace?

A: /root/lsiarray13

Q: Where are the log files located?

A: To enable logging, do the following:

Note: Changes to the tracing level requires a restart of the provider to take effect.

1. Go to the directory where SMI-S Provider is stored.

- **a.** For a Windows operating system, the directory is C:\LSI\.
- **b.** For a UNIX-based operating system, the directory is /opt/lsi/sbma/data/.

2. Edit the providerTraceLog.properties file.

- **a.** Remove the pound sign (#) from the lines containing FILE, LEVEL, and EVENTS.

3. Save the file, and exit the text editor.

4. Stop and start the CIM server by using the specific location and name.

Q: How do I change the ports that the provider binds to?

A: Go to the <installPath>\bin directory.

For a Windows operating system, the directory is c:\lsi\pegasus28\pegasus\bin

For a UNIX-based operating system, the directory is /opt/pegasus28/pegasus/bin/

Run the following commands:

cimconfig –s httpPort=<newHttpPort> -p

cimconfig –s httpsPort=<newHttpsPort> -p

Q: I keep getting a "Storage array added successfully", but instead of returning the UUID, it returns a "index string out of bounds".

A: Double check the IP address. This is the provider's way of saying, "this host is pingable, but it's not a storage array".

Q: Array does not appear to be added to the provider when editing the arrayhosts.txt file, what should I do?

A: See section above “Adding a SAN” under the “Provider Version Eagle 2 and above” section.

Troubleshooting LSI Legacy Provider (Pre-Eagle 2)

Q: What are the ports that LSI provider listens on?

A: 5988, 5989 and 2463.

The port 2463 is used to set RPC sessions to the storage controller.

Q: How do I change the port the provider listens on?

A: To change the port, do the following:

On the machine running the Provider:

Open the portInfo.properties located (by default): C:\Program Files\EngenioProvider\SMI_SProvider\bin.

Change the entry CIM-XML=5988 to the desired port which has no conflicts.

Save the changes.

Restart the Engenio SMI-S Provider Server service.

In the Profiler GUI:

Go to Administration > Hosts.

Click the monkey wrench icon for the Array.

Change the HTTP port to the port set in the portInfo.properties on Provider.

Save the changes.

Q: How do I enable logging for debugging the provider, and where is the log located?

A: To enable logging, do the following:

Note: Changes to the tracing level requires a restart of the provider to take effect.

The SMISProvider.log file is created if you have debug tracing enabled. The file could be located in the following locations:

\Program Files\EngenioProvider\SMI_SProvider\bin\

\Windows\System32\

\EngenioProvider\SMI_SProvider\bin\

If you are not able to find the SMISProvider.log file then follow the below instructions to enable debug tracing and duplicate the issue so the SMISProvider.log file is created:

1. Stop the Provider

2. Edit the providerTraceLog.properties file located in [Installation Drive]\Program Files\EngenioProvider\SMI_SProvider\bin\

3. Remove the "#" symbol from the last line of the code, which looks like:

   #log4j.logger.ProviderLog=DEBUG, File

   The line of code should now look like: log4j.logger.ProviderLog=DEBUG, File

4. Save the file

5. Restart the Provider

On UNIX: the trace log is in the {install location}/SMI_SProvider/bin directory.

Q: Why, on a minute by minute basis, am I seeing some perf stats as 0.0?
A: Because LSI only polls their arrays on a 10 minute basis. It is too taxing on the array to gather more frequently than that.

Q: How many arrays can be monitored at one time?

A: LSI recommends no more than 4 arrays at once.

The following is an excerpt from their release Notes:
"The maximum configuration recommended for the SMI provider is either 3 storage systems or a total of 512 volumes, whichever is reached first. If the limits are exceeded, the provider may not be able to generate performance statistics."

Q: What performance information is available from the LSI array and how is it obtained?

A:

Array Perf: smi-s

Controller Perf: calculated by Profiler. Aggregate the performance values for all the luns that belong to specific controller.

LUN Perf: smi-s

Disk Perf: API. Currently using the Crystal (10.10) version API. In order to ascertain disk performance from an array, the controller firmware minimum version must also be Crystal release (7.10). The 10.10 version of the API was built against jdk 1.4, which matches with the jdk used in the Profiler agent at the time of the 4.8 release. The 10.15 (Crystal maintenance) and 10.30 (Emerald) release was compiled against jdk 1.5, and is the reason it is not used.

Volume Group Perf: calculated by Profiler. Aggregate the performance values for all the luns that belong to specific raid group.

Q: Why is disk performance not showing up?

A: The controller firmware must be version 7.10 or greater. We use the API to gather the data, and there is a dependency on the controller firmware to be greater than 7.10. A trap is sent to Profiler if the minimum version is not met.

You might hear the controller versions referred to by name, which are:

6.60 - Chromium (no disk perf avail, only in this list to show firmware name)

7.10 - Crystal

7.15 - Crystal maintenance

7.30 - Emerald (which is the xbb2)

7.36 - Crystal/Emerald 4Q08 Maintenance

7.50 - Aurora (2009)

7.60 - Allegheny (2009)

8.10 - Flint (2009)

Q: Is any configuration required to get disk performance to show up?

A: No configuration required on the agent nor from Profiler gui. The disk performance uses LSI's API (symsdk.jar) in conjunction with the smi-s provider to ascertain the disk performance. The API requires the IP addresses of the controllers. The IP addresses are obtained from the smi-s provider; therefore, you must have the smi-s settings configured correctly.

Q: How do I get the LSI provider to work on Solaris?

A: For Solaris 10, you will probably need to change the port the lsi provider listens on, as solaris 10 ships w/ a cimom enabled by default that is already bound to 5988.

For solaris 10 do the following:

1. Install provider following instructions

2. Stop the provider (/opt/engenio/SMI_SProvider/bin/launch stop)

3. Change the ports in /opt/engenio/SMI_SProvider/bin/portInfo.properties to something other than 5988 and 5989. CIM-XML is listed twice, so be sure to change both

4. Check that slp is running (ps –eaf | grep slp)

a. should see /usr/java/jre/bin/java -Xmx128m -classpath /usr/share/lib/slp/slpd.jar

b. can also check the slp port is bound to by doing netstat –an | grep 427. Should see port 427 in a listen state

5. Start slp if not running (/etc/init.d/slpd start)

slp requires that the /etc/inet/slp.conf file exists. If the file does not exist, then copy the slp.conf.example file (cp /etc/inet/slp.conf.example /etc/inet/slp.conf)

6. Start the provider (/opt/engenio/SMI_SProvider/bin/launch start)

For solaris 8 or 9, you should not have to change the provider ports, as there shouldn't be a cimom running on port 5988. But you should always verify (netstat –an | grep 5988) to make sure port 5988 isn't already bound to.

Q: Provider still doesn't work on Solaris, what logs can I look at?

A: You can edit the /opt/engenio/SMI_SProvider/bin/launch script and change the PROVIDER_OUT=/dev/null to PROVIDER_OUT=$PROVIDER_HOME/SMI_SProvider/bin/provider_launch.log

You can then view the provider_launch.log and SMISProvider.log (found in /opt/engenio/SMI_SProvider/bin) to further diagnose issue

PROVIDER_OUT=$PROVIDER_HOME/SMI_SProvider/bin/provider_launch.log

Q: What is the default username/password for provider running on Solaris?

A: You must use a valid username/password that is used to login to the system

Q: How do I add an array to the provider on Solaris?

A: Run /opt/engenio/SMI_SProvider/bin/ProviderUtil

You must provide ip address of the controller, and also a valid username/password that is used to login to the system

Q: Can you use the Windows installer on a 64-bit Windows OS?

A: No. According to the LSI Representative, this will be supported in the next generation of the provider (information is as of 2/6/2009)

Q: How do I obtain the Support Bundle Data from LSI array?
A: To obtain the Support Bundle Data from Santricity/Storage Manager:

1. From the array management window (AMW), select the **Advance** drop down menu

2. Choose **Troubleshooting** and then **Collect All Support Data**.

3. From this screen, specify the location to save.

4. Click **Start**

Q: What files are needed to send a bug to LSI?

A: Any issues related to LSI provider, get the following:

- Provider logs (See 'How do I enable logging for debugging the provider, and where is the log located' for log file location)
- ArrayHosts.txt (located in C:\Program Files\EngenioProvider)
- Support Data (See question 'How do I obtain the Support Bundle Data from LSI array')
- LSI provider version info

OS Embedded Providers

Some of the OS platforms come with a cimom already installed, running, and bound to the default ports of 5988 and 5989. This section is used to describe those providers and possible ways to work around them.

Solaris

Q: What is the default cimom service on Solaris?

A: For Solaris 9 and 10, /etc/init.d/init.wbem launches the scm (Solaris Management Console), which is a bootloader for the embedded cimom smcboot (/usr/sadm/lib/smc/bin/smcboot)

Q: How do I start/stop the smcboot cimom service?

A: Solaris changed the default way services can be started/stopped in Solaris 10 (via service management facility: smf). SMF avail in Solaris 9, but became default way to handle services in Solaris 10. Below are couple methods to start/stop service using smf and not using smf.

1. To start:

/etc/init.d/init.wbem start

svcadm enable svc:/application/management/wbem

2. To stop:

/etc/init.d/init.wbem stop

svcadm disable svc:/application/management/wbem

Note: other useful smf commands:
(www.princeton.edu/~unix/Solaris/troubleshoot/smf.html)

List all services

svcs –a

Check status of service

svcs -l <service name>

example: svcs –l svc:/application/management/wbem

List properties of service

svccfg -s <service>

then at the <service name> prompt: listprop

example:

svcfg –s svc:/application/management/wbem

svc:/application/management/wbem> listprop

Q: I see port 5988/5989 is bound to, but smcboot is not running, how do I determine the process that is bound to those ports?

A: Copy/paste following script to new file on system. Script from unknown source#!/bin/ksh

```
line='--------------------------------------------'
pids=$(/usr/bin/ps -ef | sed 1d | awk '{print $2}')

if [ $# -eq 0 ]; then
  read ans?"Enter port you would like to know pid for: "
else
  ans=$1
fi

for f in $pids
do
  /usr/proc/bin/pfiles $f 2>/dev/null | /usr/xpg4/bin/grep -q "port: $ans"
  if [ $? -eq 0 ]; then
    echo $line
    echo "Port: $ans is being used by PID:\c"
    /usr/bin/ps -ef -o pid -o args | egrep -v "grep|pfiles" | grep $f
  fi
done
exit 0
```

Pillar Provider

The Pillar SMI provider is embedded in the array itself, so there is nothing a customer needs to do to install it. If a customer is running an older Pillar Axiom system that has the 512Meg Pilot hardware, the provider is by default disabled. Provider is enabled by default on systems with 2 Gig Pilots.

Pillar doesn't recommend enabling the SMI provider if the customer has the older 512 Meg Pilots and recommends that they have it upgraded to the 2 Gig versions. Customers can contact Pillar's customer support to have their systems upgraded to the 2 Gig Pilots.

The provider uses the same username/passwords that the customer has set up for their Axiom systems. Standard SLP discovery mechanism is used.

The interop namespace for the provider is /root/pg_interop, and the namespace is /root/pillar.

Upgrades for the provider are bundled with system software upgrades. Currently Pillar is SMI 1.1 certified with the 2.3 Axiom software release.

Troubleshooting Pillar

The following section list FAQs for troubleshooting a Pillar provider.

Q: Since provider is embedded in the controller, is there a way to manually start/stop the provider? If so, how?

A: You can restart the provider two different ways (force a Pilot failover, or issue disable/enable startup command for smi provider) both of which require that the Support Tool be licensed and the supporttool software be locally installed.

You can get a list of the support tool commands with “supporttool.exe help list-requests > requests.txt”

For a quick syntax of any command, use “supporttool.exe template –d [command name]”

Restart smi provider using one of two avail methods

Using Support Tool to force a Pilot Failover.

This is completely non-disruptive to the data path, it issues a Linux reboot to the active Pilot, which does a failover to the passive, and in the process starts the web service and SMI-S Provider service on the standby pilot.

Warning: Do not do this if there is a storage resource modifying task in progress.

$ supporttool.exe sub -u pillar -p a1s2d3f$ -H [your pilot hostname or shared IP] ForcePilotFailure

You should get a response that looks like this:

- Header
- ProtocolVersion: 0.1
- SessionKey: 7cc6935085aac74cda7d19a1d3f250fc
- Time: 2009-07-28T15:40:50-07:00
- ClientData: supporttool
- RequestStatus: Succeeded
- Error List
- ForcePilotFailureResponse
- Within a minute or two, you should be able to get back into the GUI as the standby pilot begins coming up.
- Using Support Tool to disable/enable the provider
- suporttool.exe PerformDisableSMIStartup
- supporttool.exe PerformEnableSMIStartup

Q: Are there log files for the provider? If so, where are they located?

A: They are located on the pilot (if you can ssh to it) under /var/log. They can be obtained via "Collect System Information" under the "Support" tab. The tar you download will have the cimserver logs.

Q: When encountering smi-s issues, what information should we collect from customer's environment?
The System information logs. See above on how to obtain logs

Q: Where can one find exact array model info?
A: On the GUI, the System -> Summary page will provide you with the Model Number as AX300 or AX500 etc.

Q: When getting version of the smi-s, is that the slammer, pilo, or brick version when going to Axiom One web gui under support?
A: Pilot OS is the version to use. For example, if you're asked to be on version 3.3, it should show up as 03.03.XX

Q: What's the minimum version of the provider we should attempt to ascertain data from?

A: 03.03.15

Q: Is performance information available? If so, what metrics?

A: Yes. Only Lun performance is available as of the 03.03.15 Pilot release

Note: Per email from Shaq from Pillar on 09/14/09: For the statistics - we're probably going to be limited to Lun and filesystem statistics for the near future. We have plans to incorporate the remaining statistics in the release 5.x timeframe but that is a ways off

Q: What Pillar licenses are required to collect valid set of smi-s data?

A: At a minimum need either Fibre Channel Protocol or iSCSI Protocol

Q: What is the default username and password for AxiomONE Storage Services Manager web gui?

A:

administrator / pillar - for admin level privileges

pillar / a1s2d3f$ - for support level privileges

Q: What license are available for the Pillar array?

A: Licensed Features

1MB Stripe
CIFS
Clone FS

Clone LUN
Fibre Channel Protocol
NDMP
NFS
Pilot SSH Access [for support use]
Pooled RAID10
SNMP
SecureWORMfs
Snap FS
Support Tool [for support use]
Thin Provisioning: FS
Thin Provisioning: LUN
Virtual Tape Library
Volume Backup
Volume Copy and Backup
iSCSI Protocol

Sun Storage TEK 99xxSeries Provider

Sun/StorageTek 99xx Series can be monitored from any OS agent by polling a HDS SMI-S Provider, typically the HiCommand Device Manager. For more information refer to the "Hitachi Data Systems (HDS) Provider section on page "179".

Sun Storage TEK 2K, 6K & FLX Provider

The Sun Storage Tek 2K, 6K and FLX Series providers utilize the LSI Provider. For more information see the "LSI Provider" section on page "233".

SMI-S Provider Tools

The following tools can be used to log into a Provider to view information regarding the arrays. This section covers how to test a provider.

There is a special EMC test provider tool.

Confirm Provider

The Array Identifier can be found using the “Test Provider” button found on the smi-s configuration page.

This button serves several purposes:
1. Verifies connectivity to provider by checking:
    a. username/password
    b. namespace
    c. provider ip address
    d. provider http/https ports
2) Default enumeration of CIM_ComputerSystem so identifier can be easily obtained
3) Ability to enumerate on any cim class for verification (like cim_blockstoragestatisticaldata to know what perf data is avail)
4) If LSI array automatically detect eagle provider and change namespace from /root/lsissi11 to /root/lsiarray13

When new smi-s device created, you can specify the username, password, and provider ip, then click the "Confirm Provider". Once credentials, ip, port verified, results of the enumeration of cim_computersystem are displayed. You can then copy/paste the desired identifier in the configuration

TestProvider (CLI interface)

Starting with Profiler version 4.6.1, the Array Identifier can be found using Profiler. This is also a good way to test connectivity to a provider.

Logging In:

1. Open command prompt.

2. Navigate to mod.sys.smis.Smis_1.0 directory in Profiler.

3. Run following command:

a. TestProvider.bat (for windows)

b. TestProvider.sh (for unix systems)

The scripts will run for both the Profiler Server and Profiler Agent.

For Unix systems, you will first have to make the script executable by issuing:

1. chmod 755 TestProvider.sh

If encountering issues try these steps:

1. Run the TestProvider manually

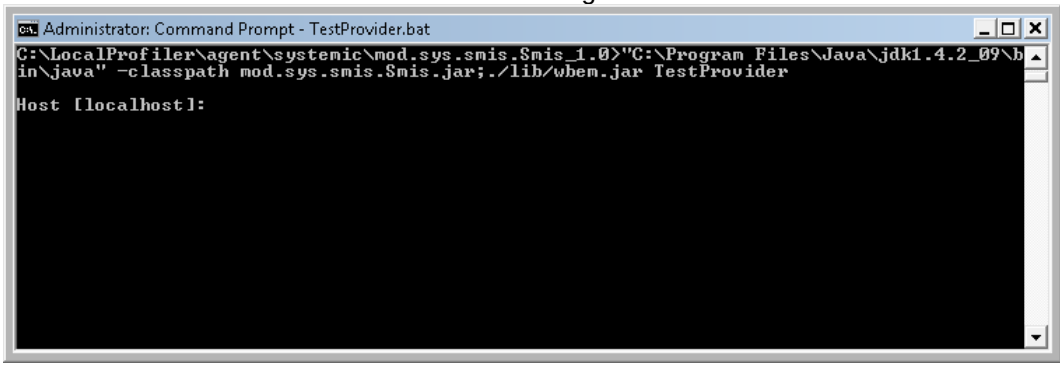
2. Pre-4.9.0 agent (uses wbemservices cim-client api)
<java bin dir>\java –classpath mod.sys.smis.Smis.jar;.\lib\wbem-1.1.jar;..\..\lib\core.jar mod.sys.smis.util.TestProvider

3. Post-4.9.0 agent (uses sblim cim-client api)

<java bin dir>\java -classpath .;mod.sys.smis.Smis.jar;.\lib\sblim-cim-client2-2.0.9-INTERNAL-r1.jar;..\..\lib\core.jar TestProvider

Note: on Unix, use colons (: and /) instead of semi-colons (; and \) when separating the list jar files above

4. You should see a screen like the following:


Administrator: Command Prompt - TestProvider.bat
C:\LocalProfiler\agent\systemic\mod.sys.smis.Smis_1.0>"C:\Program Files\Java\jdk1.4.2_09\bin\java" -classpath mod.sys.smis.Smis.jar;./lib/wbem.jar TestProvider
Host [localhost]:

5. Fill in the information below to log into the provider. (All defaults are in brackets. To accept default, simply leave field blank and hit return).

a. Host – Hostname or IP of provider you wish to connect to.

b. Port – Port the provider is listening on (defaults are 5988 for http and 5989 for https).

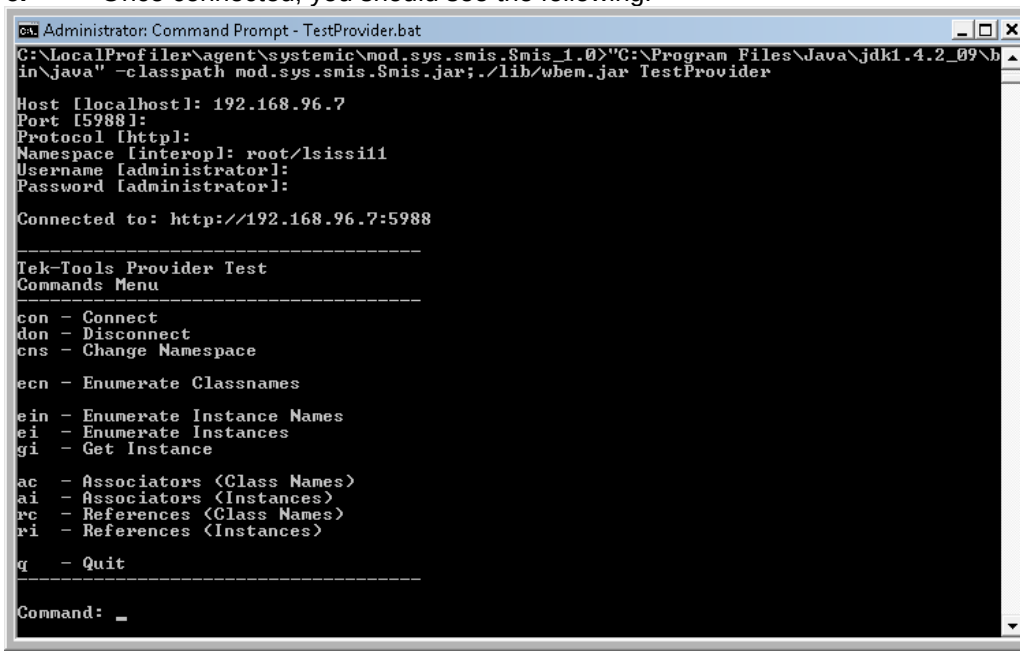
c. Protocol – Either http or https (any other text, default http will be used).

d. Namespace – Cimom namespace to connect to (refer to Default Namespace section for the vendor's default namespace).

e. Username – Username for provider.

f. Password – Password for username above for provider.

6. Once connected, you should see the following.

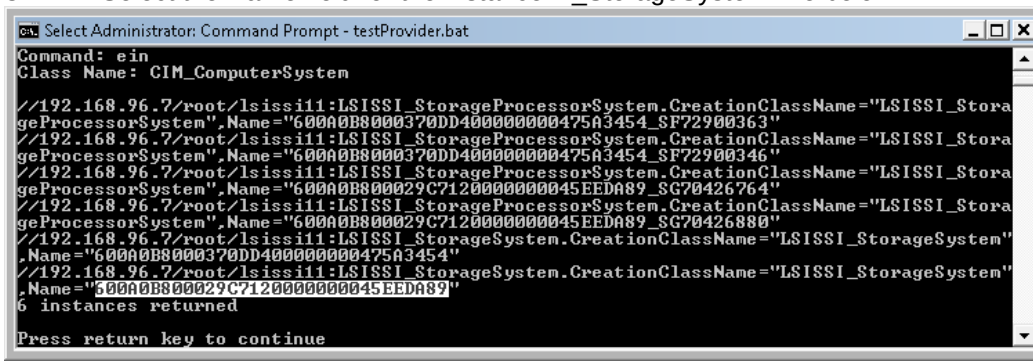


Obtaining Array Identifier (enumerating instances)

1. Type ein at command prompt.

2. Type CIM_ComputerSystem at Class Name prompt.

3. Select the Name field for the instance if _StorageSystem like below.



CIMWorkshop

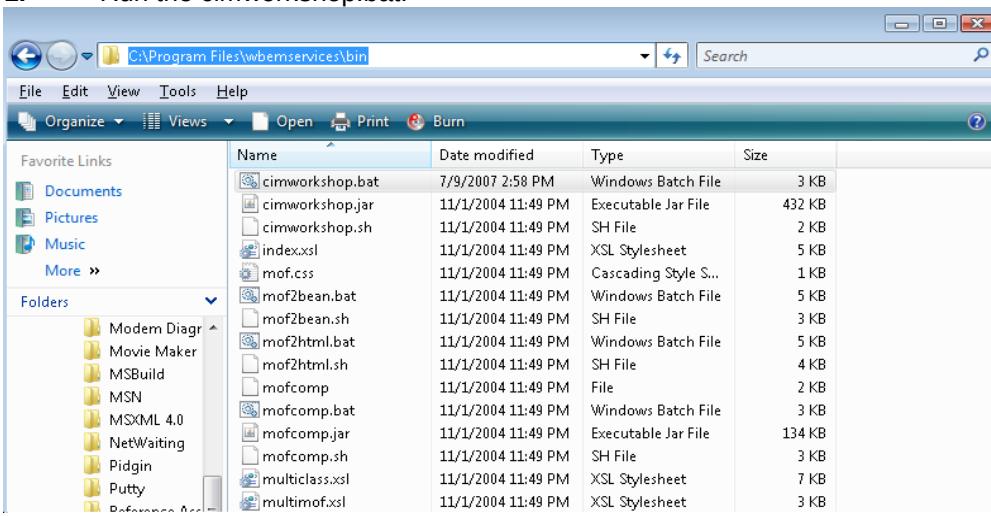
Download: http://sourceforge.net/project/showfiles.php?group_id=26421

Installation

1. **Unzip the wbemservices-1.0.2.bin.zip**
2. Open the wbemservices-1.0.2.bin directory.
3. Edit cimworkshop.bat located in the bin directory.
   a. Un-REM line 36, and change the path to the directory where the java jre is installed, if JAVA_HOME is not set as a global environment variable Example: set JAVA_HOME=C:\Progra~1\Java\jre1.6.0.

Obtaining Array Identifier

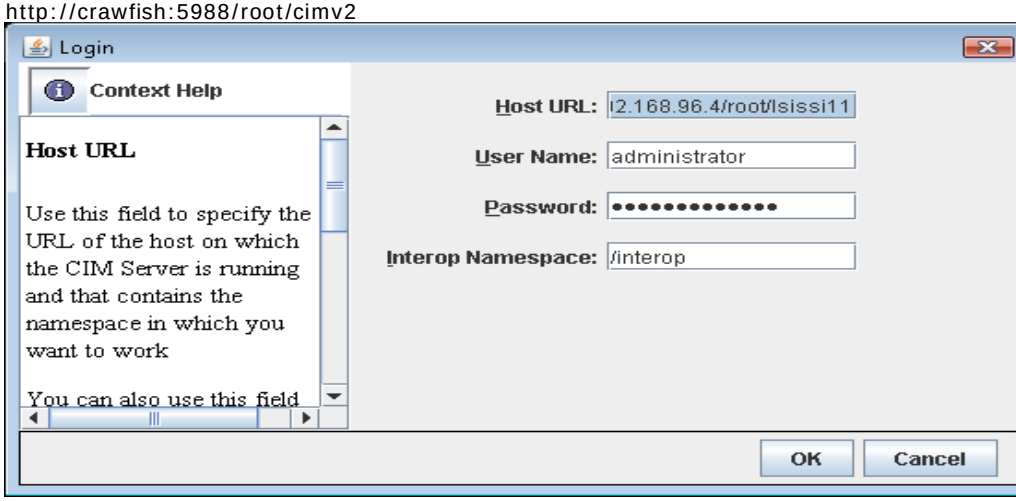
1. Run the cimworkshop.bat.


C:\Program Files\wbemservices\bin
Search
File Edit View Tools Help
Organize Views Open Print Burn
Favorite Links
Documents
Pictures
Music
More
Folders
Modem Diagr
Movie Maker
MSBuild
MSN
MSXML 4.0
NetWaiting
Pidgin
Putty
Name Date modified Type Size
cimworkshop.bat 7/9/2007 2:58 PM Windows Batch File 3 KB
cimworkshop.jar 11/1/2004 11:49 PM Executable Jar File 432 KB
cimworkshop.sh 11/1/2004 11:49 PM SH File 2 KB
index.xsl 11/1/2004 11:49 PM XSL Stylesheet 5 KB
mof.css 11/1/2004 11:49 PM Cascading Style S... 1 KB
mof2bean.bat 11/1/2004 11:49 PM Windows Batch File 5 KB
mof2bean.sh 11/1/2004 11:49 PM SH File 3 KB
mof2html.bat 11/1/2004 11:49 PM Windows Batch File 5 KB
mof2html.sh 11/1/2004 11:49 PM SH File 4 KB
mofcomp 11/1/2004 11:49 PM File 2 KB
mofcomp.bat 11/1/2004 11:49 PM Windows Batch File 3 KB
mofcomp.jar 11/1/2004 11:49 PM Executable Jar File 134 KB
mofcomp.sh 11/1/2004 11:49 PM SH File 3 KB
multiclass.xsl 11/1/2004 11:49 PM XSL Stylesheet 7 KB
multimof.xsl 11/1/2004 11:49 PM XSL Stylesheet 3 KB

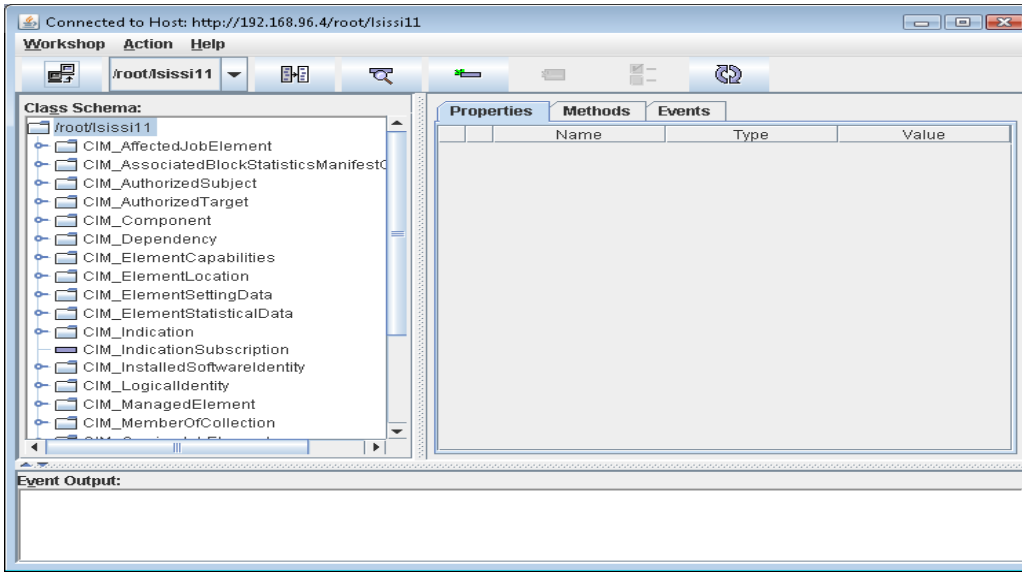
2. Enter the Host URL, User Name, and Password for the Array.

Host URL Example:

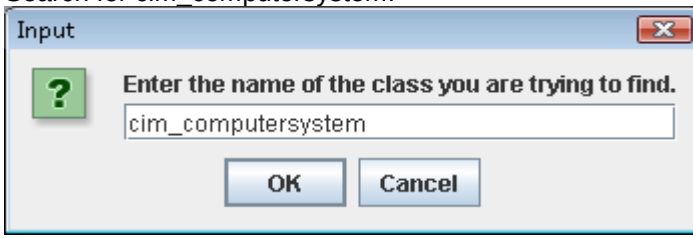
If you wanted to connect to the namespace root/cimv2 on the host named crawfish using http on port 5988, you would specify the host as:
http://crawfish:5988/root/cimv2



3. Click **OK**. You will be taken to screen below:

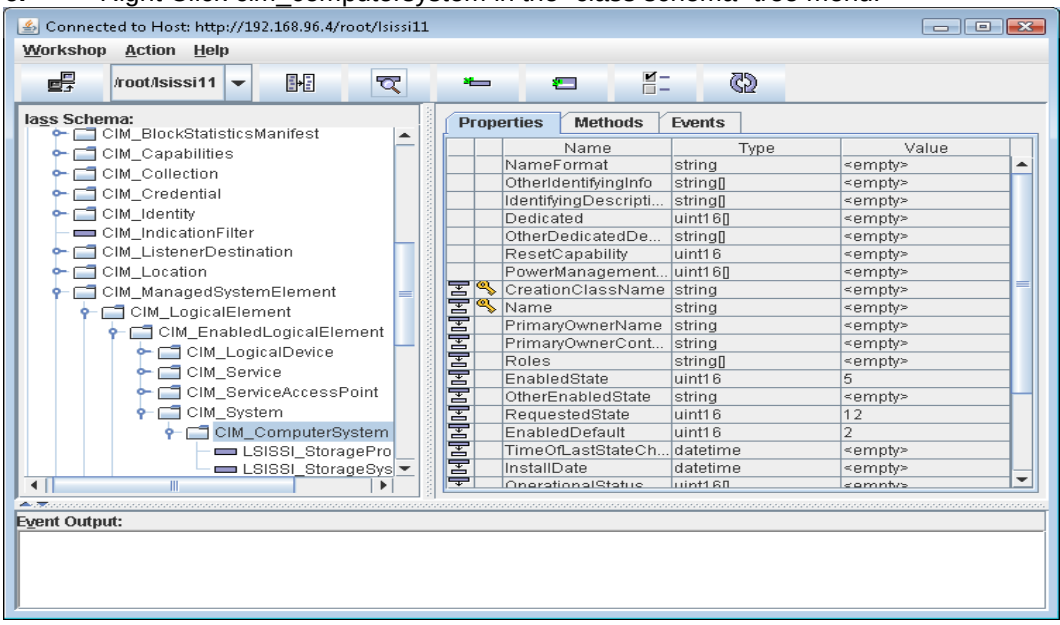


4. Click the Magnifying Glass looking icon or Action > Find Class. Search for cim_computersystem.

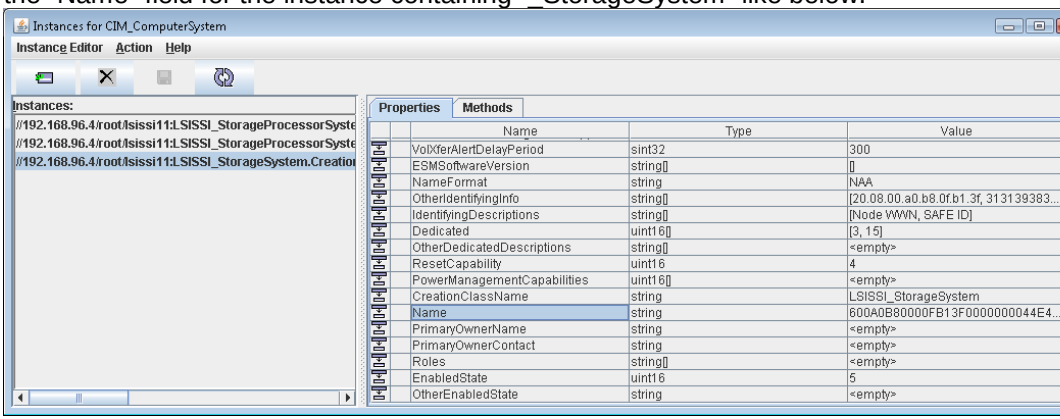


5. Click **OK.**

6. Right Click cim_computersystem in the “class schema” tree menu.



7. Click “Show Instances”. You will find the Array Identifier / WWN under the “Name” field for the instance containing “_StorageSystem” like below.



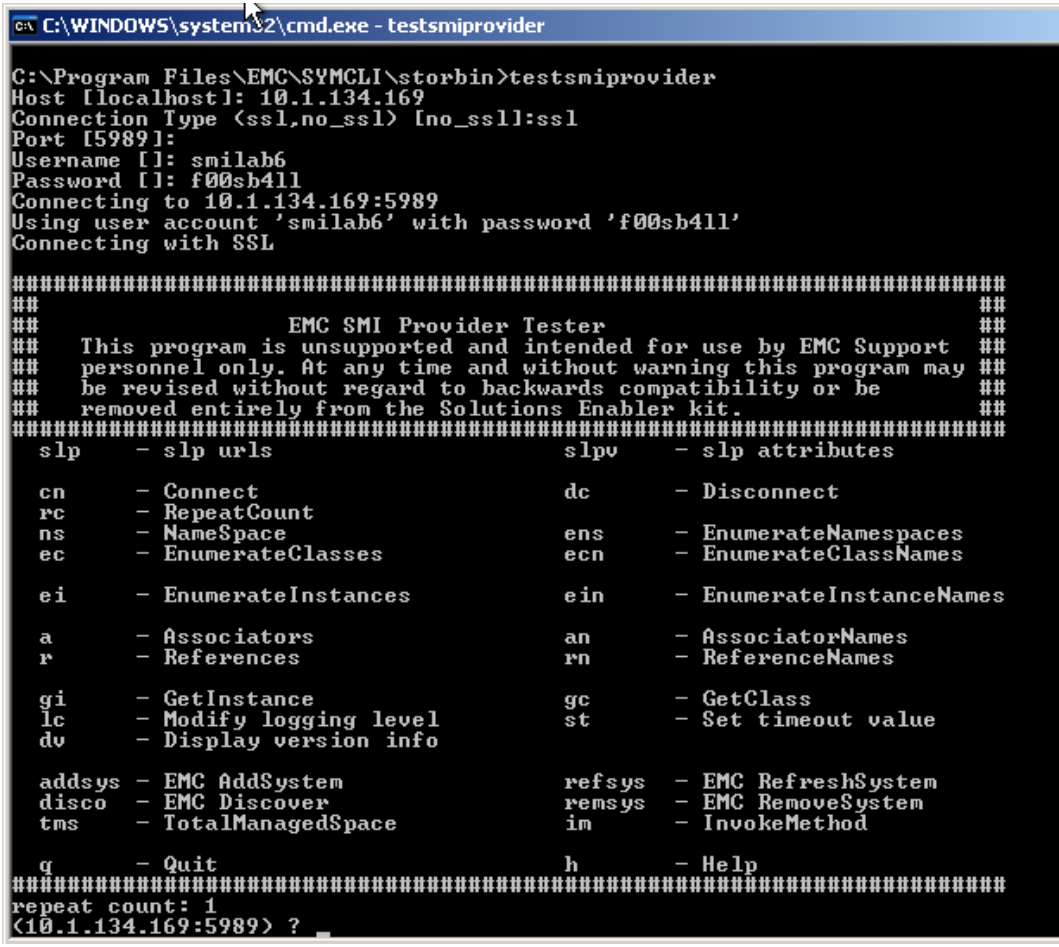
EMC TestSMIprovider

Installation

Follow the instructions in the EMC Provider > Installation section on where to download and how to install this utility.

Obtaining Array Identifier

1. Log into the remote Array using the Host, Connection Type, Port, Username and Password.


C:\WINDOWS\system32\cmd.exe - testsmiprovider
C:\Program Files\EMC\SYMCLI\storbin>testsmiprovider
Host [localhost]: 10.1.134.169
Connection Type (ssl,no_ssl) [no_ssl]:ssl
Port [5989]:
Username []: smilab6
Password []: f00sb4ll
Connecting to 10.1.134.169:5989
Using user account 'smilab6' with password 'f00sb4ll'
Connecting with SSL
EMC SMI Provider Tester
This program is unsupported and intended for use by EMC Support personnel only. At any time and without warning this program may be revised without regard to backwards compatibility or be removed entirely from the Solutions Enabler kit.
slp - slp urls
slpv - slp attributes
cn - Connect
dc - Disconnect
rc - RepeatCount
ns - NameSpace
ens - EnumerateNamespaces
ec - EnumerateClasses
ecn - EnumerateClassNames
ei - EnumerateInstances
ein - EnumerateInstanceNames
a - Associators
an - AssociatorNames
r - References
rn - ReferenceNames
gi - GetInstance
gc - GetClass
lc - Modify logging level
st - Set timeout value
dv - Display version info
addsys - EMC AddSystem
refsys - EMC RefreshSystem
disco - EMC Discover
remsys - EMC RemoveSystem
tms - TotalManagedSpace
im - InvokeMethod
q - Quit
h - Help
repeat count: 1
(10.1.134.169:5989) ?

2. Type “ens” to get a list of namespaces.

```
################################################################################
repeat count: 1
(10.1.134.169:5989) ? ens
++++ Testing Namespace operations ++++
Enumerate 4 Namespaces; repeat count 1; in 0.1875 seconds
__Namespace.Name="PG_InterOp"
__Namespace.Name="PG_Internal"
__Namespace.Name="cimv2"
__Namespace.Name="eva"

In 0.296875 Seconds

Please press enter key to continue...
```

3. Type “ns” to change namespaces

Note: the default namespace for this utility is root/emc. If working with non-EMC arrays, use the default namespace for that array.

```
################################################################################
repeat count: 1
(10.1.134.169:5989) ? ns
Namespace [root/emc]: root/eva
```

4. Type “ein” to enumerate instance names.

Note: This will give us a list of all of the instances for a particular class.

5. Type “cim_computersystem” for the list of Arrays the Provider is monitoring.

```
################################################################################
repeat count: 1
(10.1.134.169:5989) ? ein
Class: cim_computersystem
++++ Testing EnumerationInstanceNames: cim_computersystem ++++
Enumerate 1 instance names; repeat count 1; in 11.515625 seconds
Instance 0:
HPEVA_StorageSystem.CreationClassName="HPEVA_StorageSystem",Name="50001FE1
E0"

In 11.734375 Seconds

Please press enter key to continue...
```

Note: In this particular example, there is only one instance, so it is easy to determine the correct identifier for the Array. For the instance containing “_StorageSystem”, the string after the word “Name” contains the Array Identifier / WWN. In this case the Array Identifier is 50001FE15000A7E0.

EMC Provider password Reset

Steps to reset EMC Provider password for v4.1.x:

1. Shutdown ECOM

2. Go to <ECOM Install directory>/conf/cst/

3. Remove RoleData.xml, LocalDirectoryData.xml, csp.clb*

4. Restart ECOM

Remote Agent Upgrade Utility

Note: This section only applies if your agents are older than version 4.12.

In the legacy product, Profiler 4.12, the improvements made to the application cannot be pushed via the upgrade module method used in previous releases. This means that all existing agents have to be upgraded in one of two ways:

1. Manually upgrade the agent via the software install. This means you will need to copy the install file to each server.
2. Use the new Remote Agent Upgrade Utility to upgrade agents remotely.

The Remote Agent Upgrade Utility is located in the additional components section of your customer portal and is intended for customers who wish to upgrade their agents remotely. The option to run the Profiler installer on each server to upgrade your agents is still viable.

This utility performs an upgrade on all agents with an assigned license. To prevent the utility from upgrading a particular agent, simply deselect the "**License**" checkbox located on the associated agent's edit page before running the upgrade script.

The following section details the agent upgrading process.

To download the Agent Upgrade Utility:

1. Download the Agent Upgrade Utility located in the **Additional Components** section of the customer portal.
2. Extract the entire file contents from the zip. The utility must be executed from the STM Server.
3. Download the new Agent images into the STM Server root directory. (C:\Program Files\SolarWinds\Profiler Server)

Performing an Agent Upgrade:

The utility must be executed from the STM Server. Keep all STM services running during the process.

To perform a bulk agent upgrade:

1. Run the following script:
   a. `Windows -> upgrade.bat`
   b. `Unix -> upgrade.sh`
2. Follow the onscreen prompts.

The utility will provide a log directory to monitor the upgrade progress.

Note: Before installing an agent you need to edit the Default Policy for Operating Systems on the server, as these settings will be pushed out to the agent when it self-registers. Once you have installed the agent, the agent will self-register and self-configure. The self-registration process will create an OS Device on the STM server. Devices can also be defined manually.

How to enable SSL login for the STM website

1. Generate a Keystore using the following command: *C:\Program Files\SolarWinds\Profiler Server\jre\bin\keytool -genkey -alias tomcat -keyalg RSA.*
2. Provide the password (no quotes): "changeit".

Note: If `changeit` is not used, find the password in the server.xml

Default location: C:\Program Files\SolarWinds\Profiler Server\conf.

3. Modify server.xml (Default location: C:\Program Files\SolarWinds\Storage Manager Server\conf).
   a. Comment the non-SSL enabled connector tag:

```
Connector port="9000" maxThreads="150"
   minSpareThreads="25" maxSpareThreads="75"
   enableLookups="false" redirectPort="8443"
   acceptCount="100" debug="0" connectionTimeout="20000"
   disableUploadTimeout="true"
```

   b. Uncomment the SSL connector tag and change the port from 8443 to 9000

c. Update this with the keystore File location `(keystoreFile=[Path To File] ): Connector port="9000" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" enableLookups="false" disableUploadTimeout="true" acceptCount="100" debug="0" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile=[Path To File]`

4. Restart the `STMWebServer` service.

Installing Local Help Files

Some users may need to host the Help files on their own web server. The following section details how to configure your STM installation to use local help.

The web properties file contains the URL location of the server where online help for SolarWinds products are stored. The default location is http://www.solarwinds.com/support/storage/storagemanager/default.htm?context=StorageManager

If you are in an Internet-restricted network environment but require access to online help, download the entire online help, copy it to a web server, and then change the Help Server URL to that of the web server. You can download the online help from http://www.solarwinds.com/support/Storage/storagemanager/docs/STMLocalHelp.zip.

To install local help.

1. Navigate to `C:\Program Files\SolarWinds\Storage Manager Server\webapps\ROOT\bin server.properties`
2. Edit the entry > `onlineHelpURL=` by entering the location of your web server.
3. Restart the webservice after the change.

General Troubleshooting

For further information about troubleshooting STM issues reference the SolarWinds Knowledge Base system located http://knowledgebase.solarwinds.com/kb/

If you need further assistance you can contact support (requires valid maintenance).
http://www.solarwinds.com/support/ticket/

Index

A
adding scripts 78
agent
  installation 15
  upgrade utility 15
asset
  change rule 77
C
configuring Profiler 19
D
data retention policies 39
database
  backup 18
  Profiler 18
deactivating
  polling 26
defining threshold rules 67
directory analysis rules 72
E
editing scripts 78
external scripts 78
F
file analysis rules 68
file type groups
  creating 65
  editing 65
G
Getting Started Page 19
groups
  creating 63
  managing 62
  using 60
L
list
  policy 27
M
managing rules 75
N
NetAPP file analysis 70
network devices
  adding 23
network discovery 23
non-windows installation
  requirements 81
O
OS device configuration 16
P
policy
  creating 28
  editing 29
product feature requests 80
product feedback 80
Profiler
  architecture 9
  installation 12
  licensing 15
  policies 26
  system requirements 13
profiler introduction 9
Profiler Server installation 13
R
reporting product bugs 80
reports
  creating 58
  deleting 59
  managing 56
  running 57
  schedule list 60
  scheduler 59
requesting product features 80
devices
  adding 24
  editing 24, 25
rule name 77
rule parameters 77

rules and alerting 66
S
scheduling rules 77
server
  setup 30
SMI-S Provider Installation 42
  CLariion arrays 47
  LSI arrays 43
  NetApp Ops Mgr 51
status
  agent 26
storage monitoring 42
sub-groups
  creating 65
T
threshold rules 72
U
user accounts
  adding 20
  editing 22
  managing 20
  overview 20
W
web console 41
windows event log rule 71